

FIG. 1

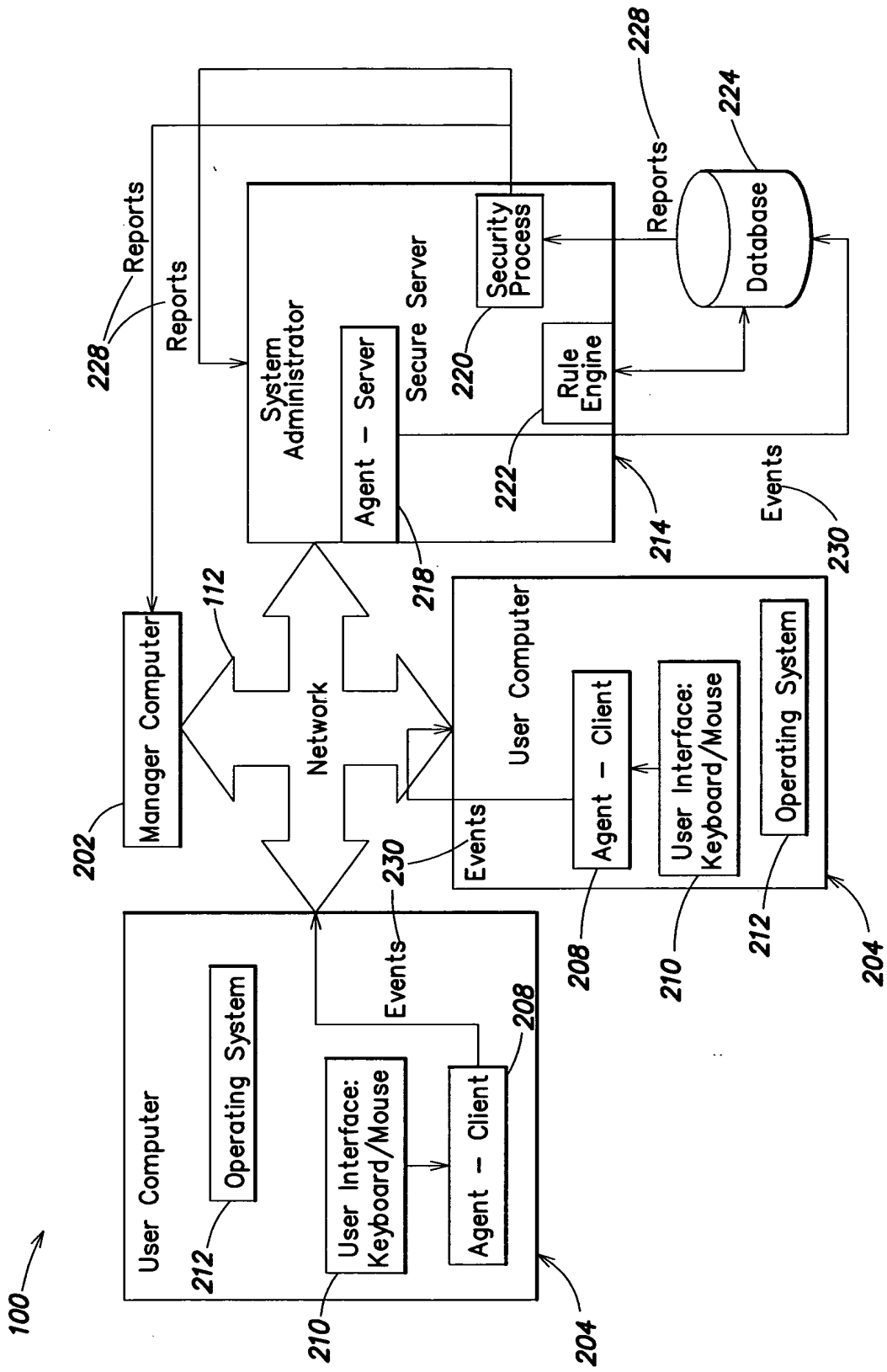


FIG. 2

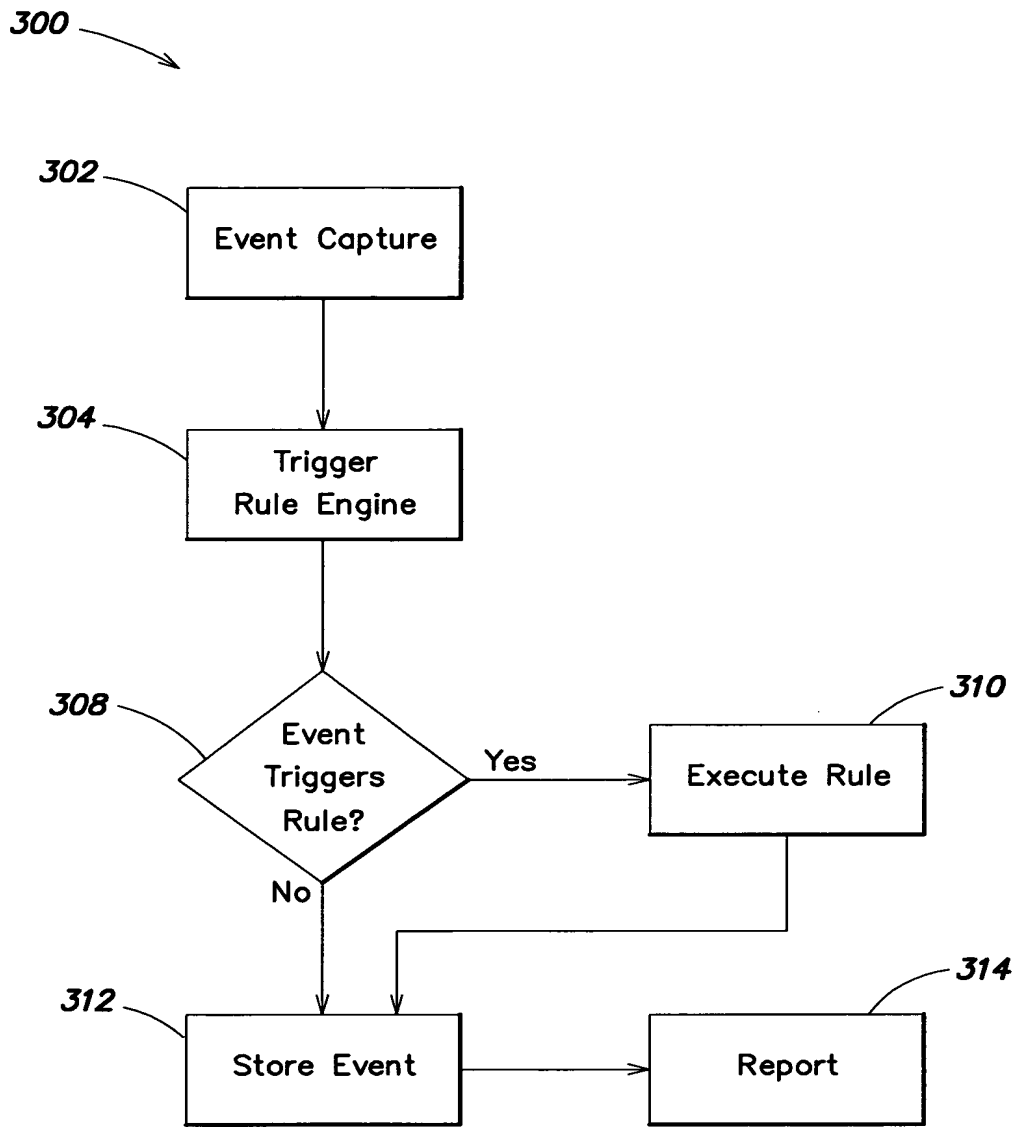


FIG. 3

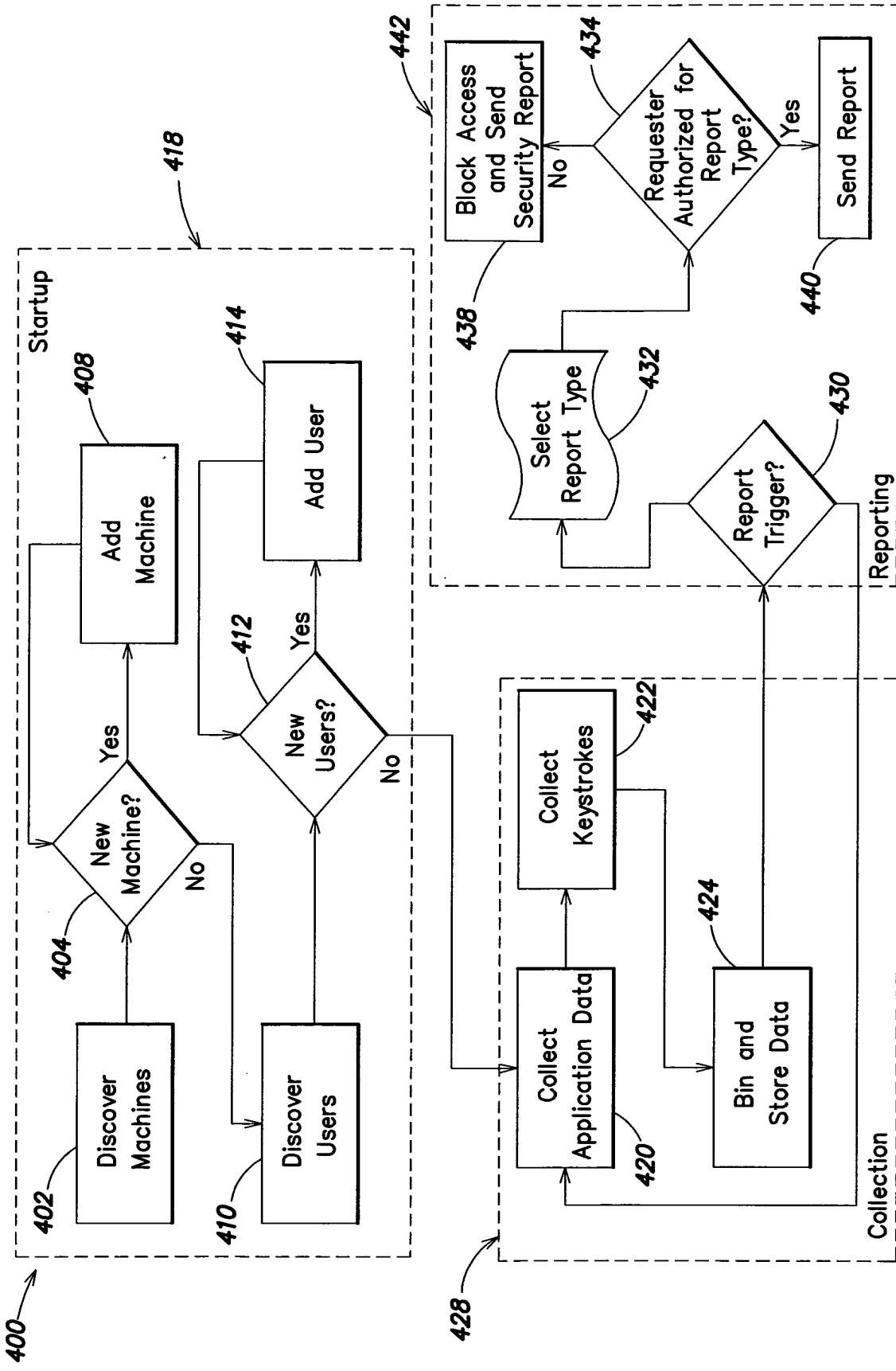


FIG. 4

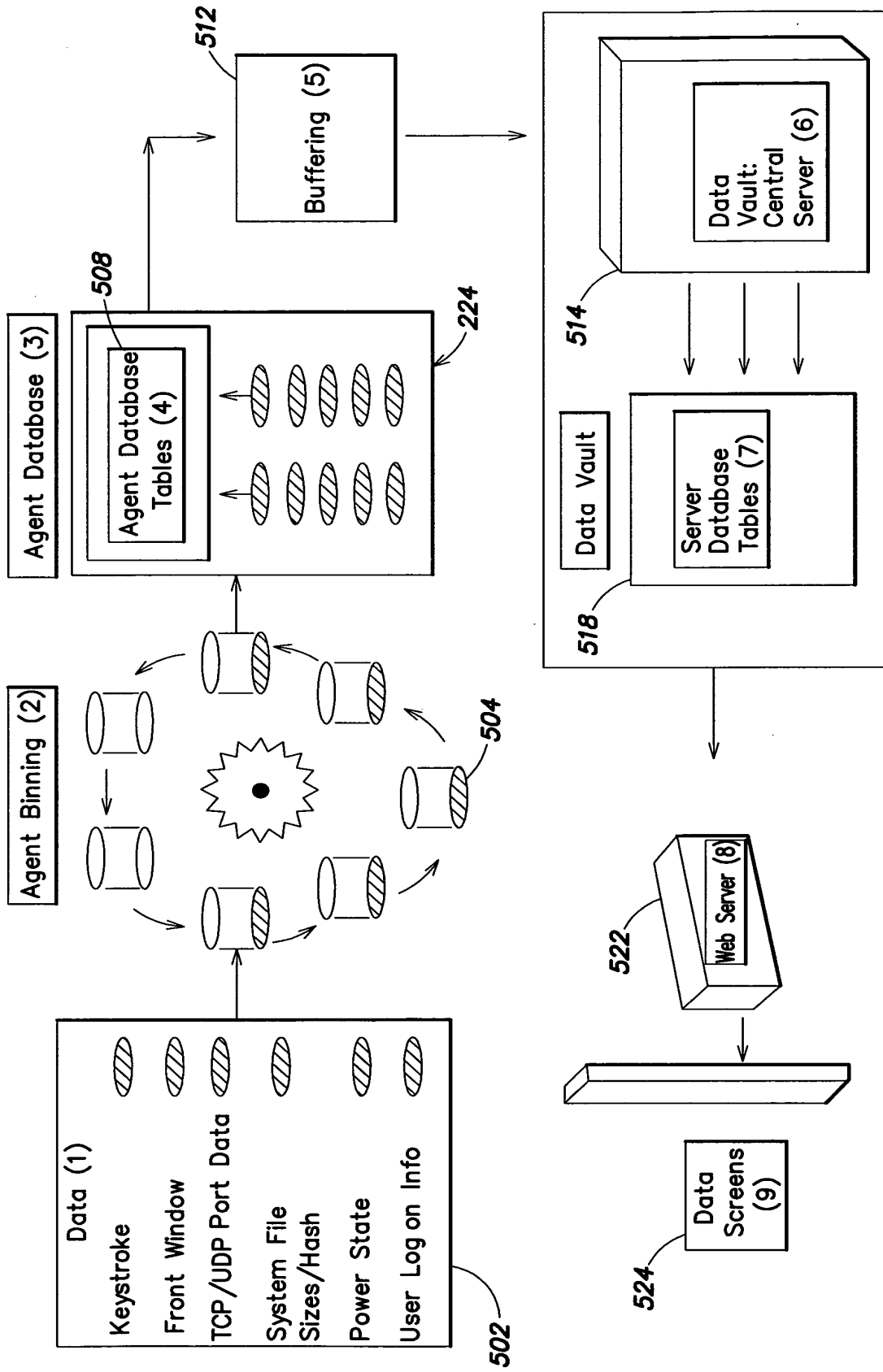


FIG. 5

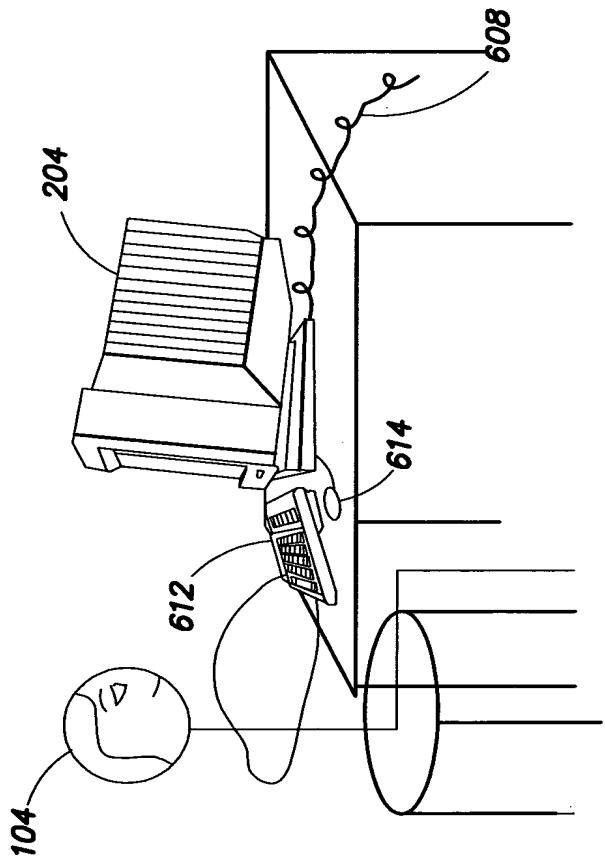


FIG. 6

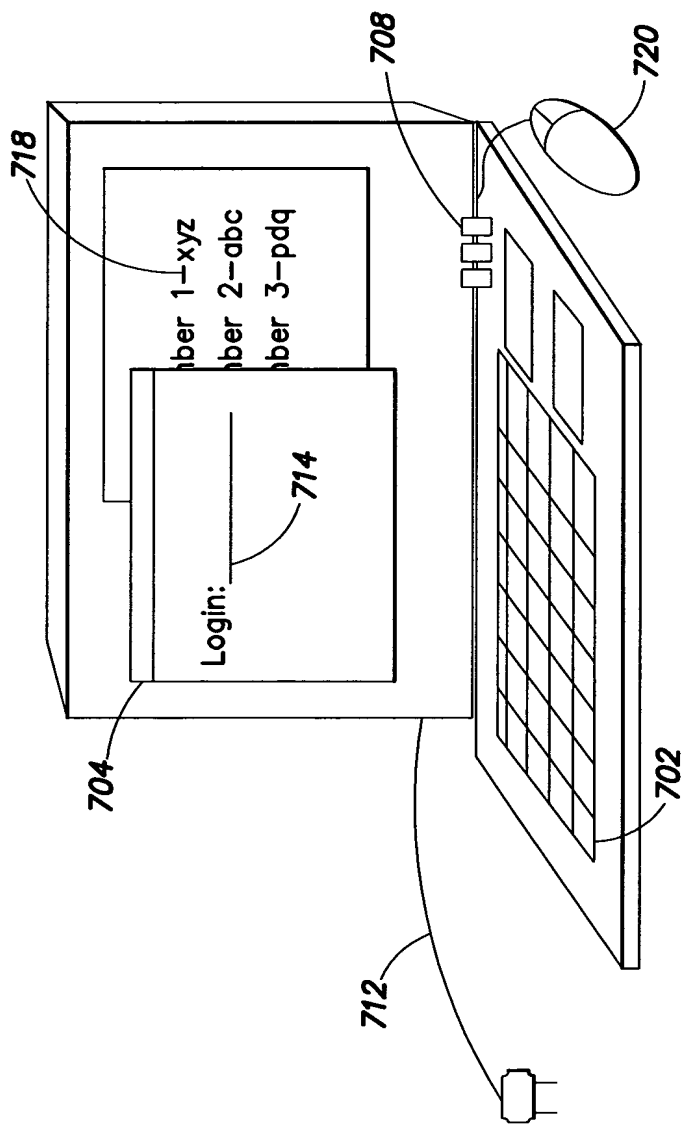


FIG. 7

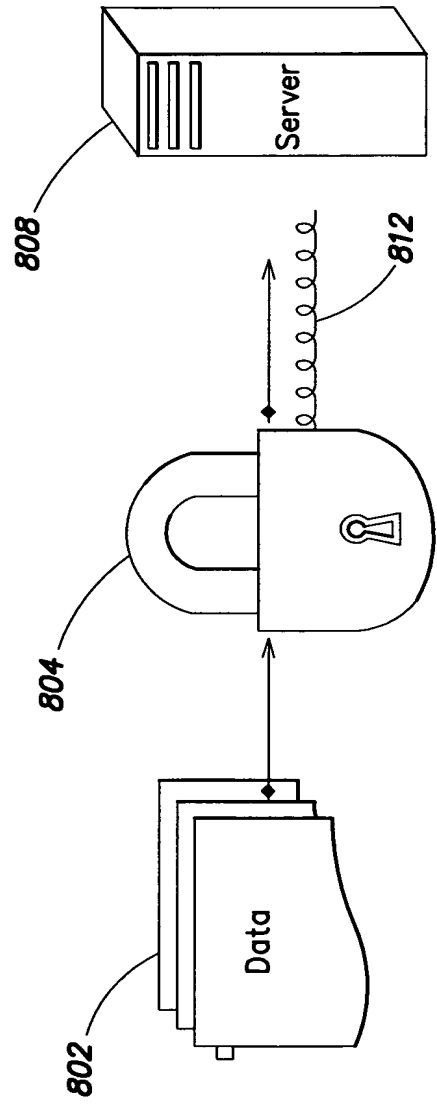


FIG. 8

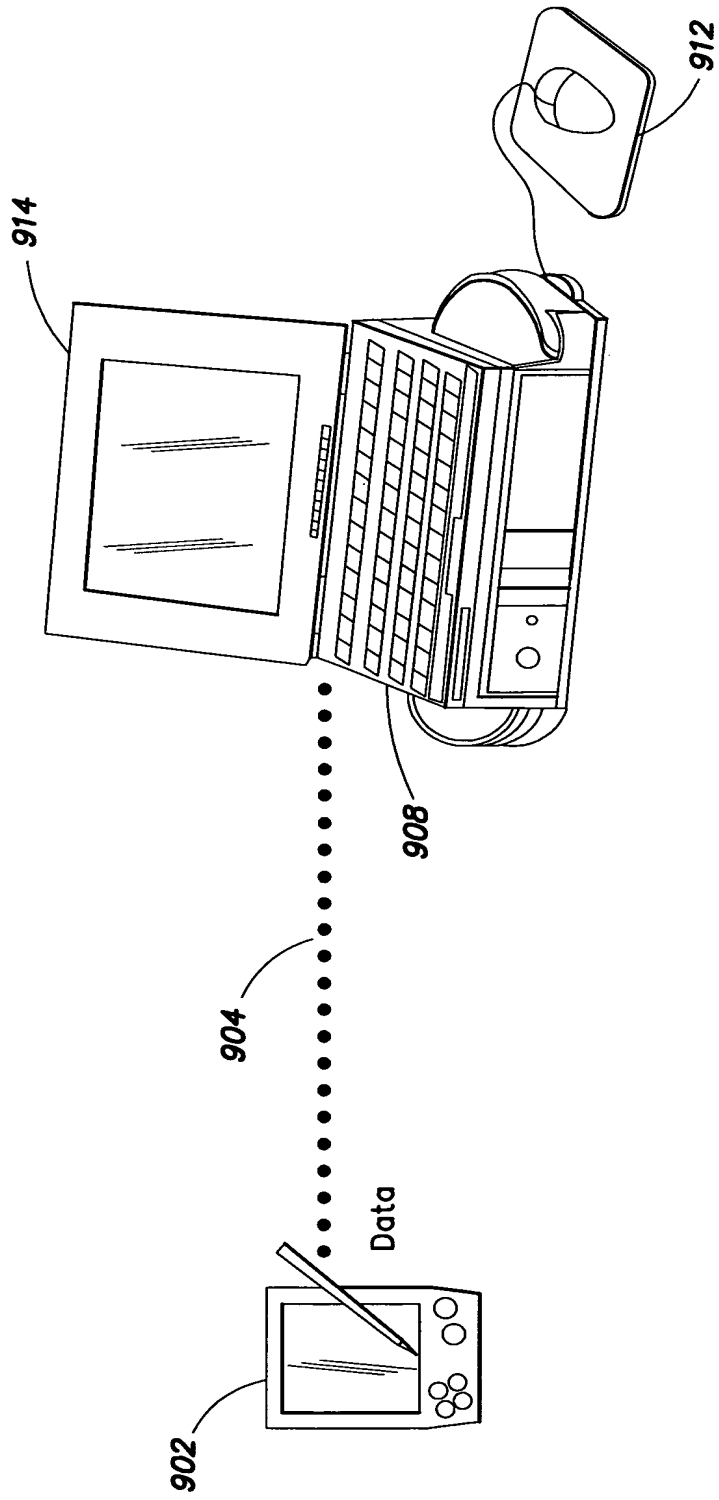


FIG. 9

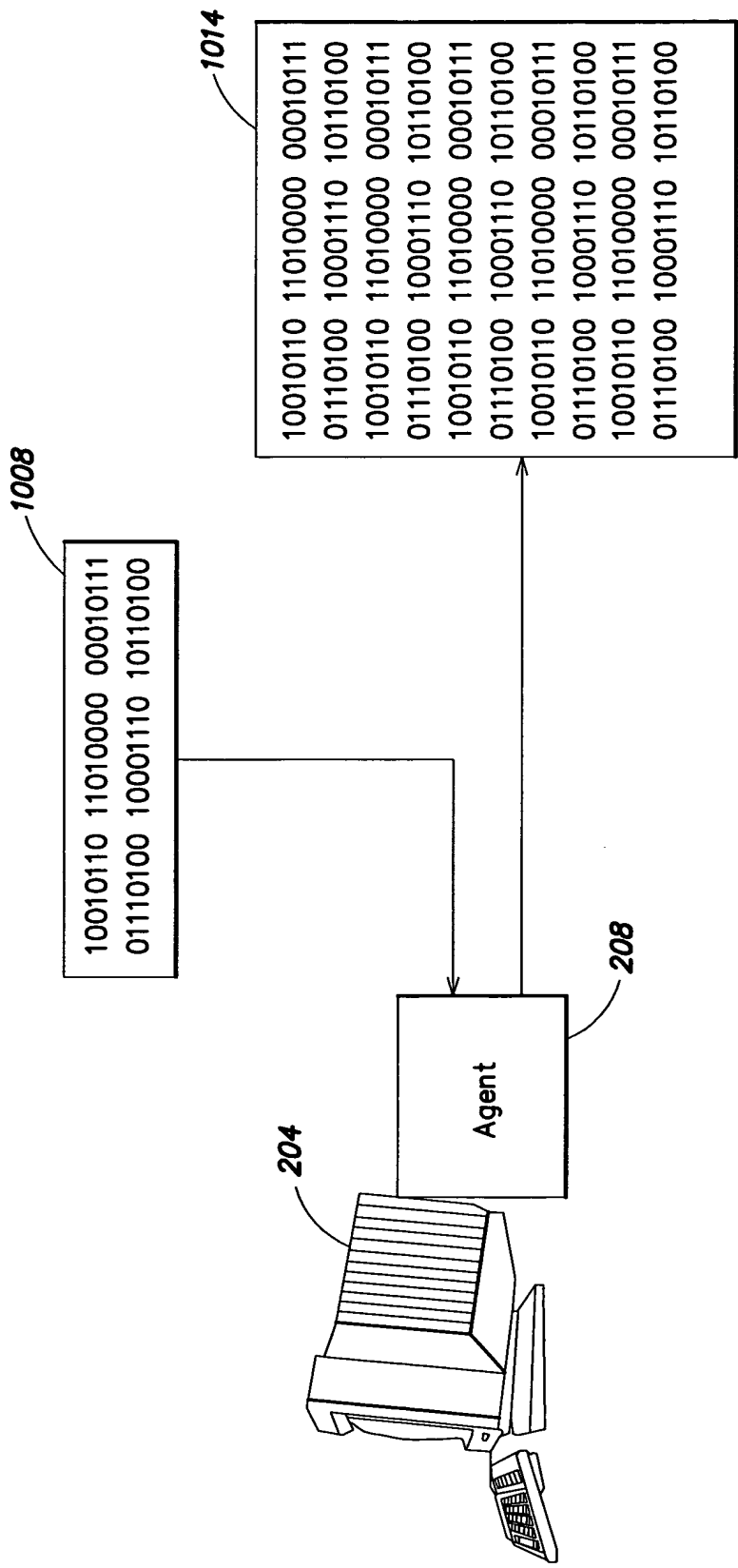


FIG. 10

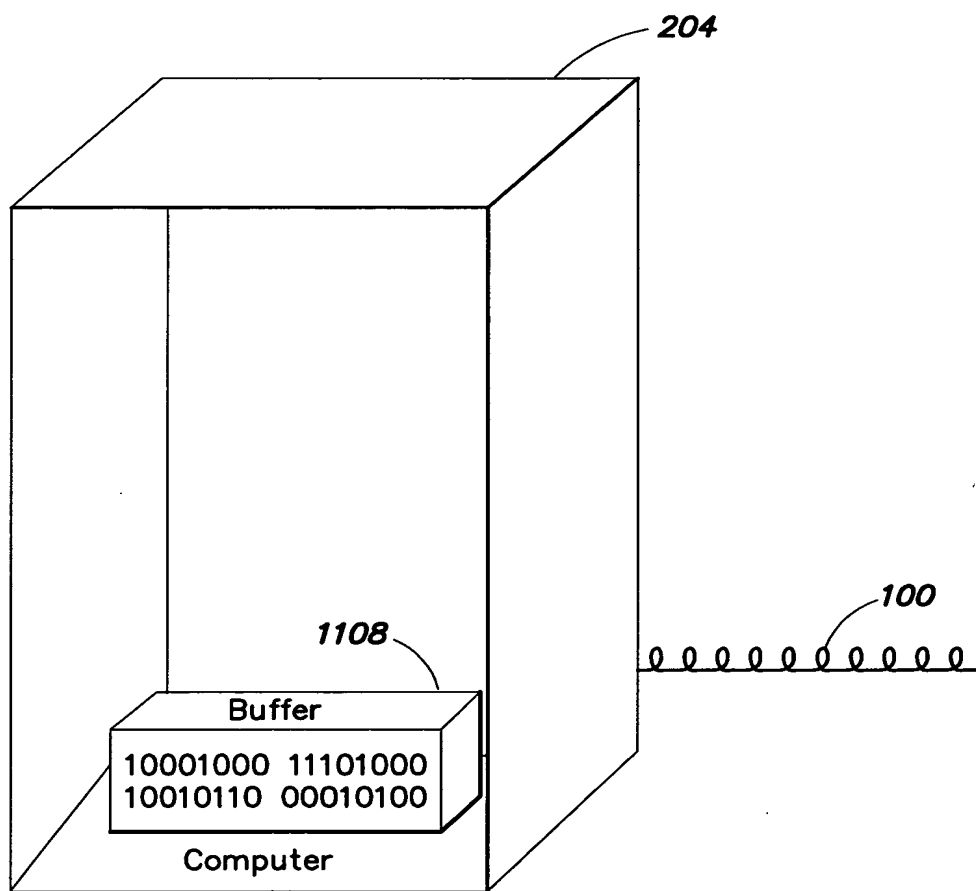


FIG. 11

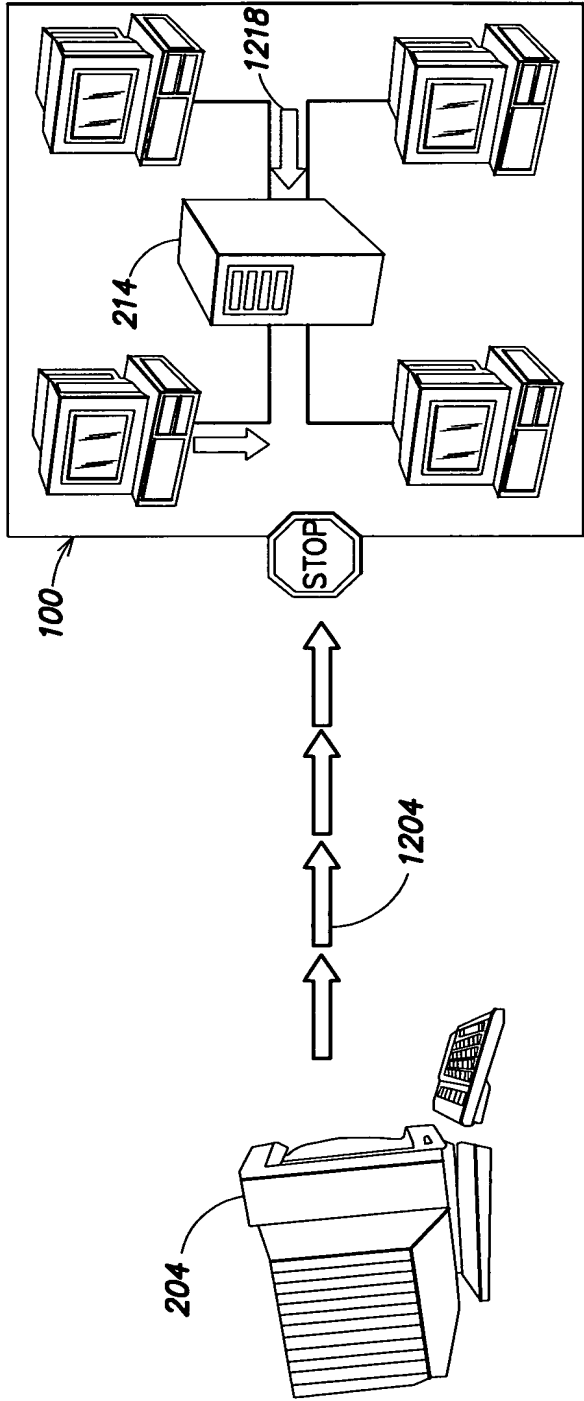


FIG. 12

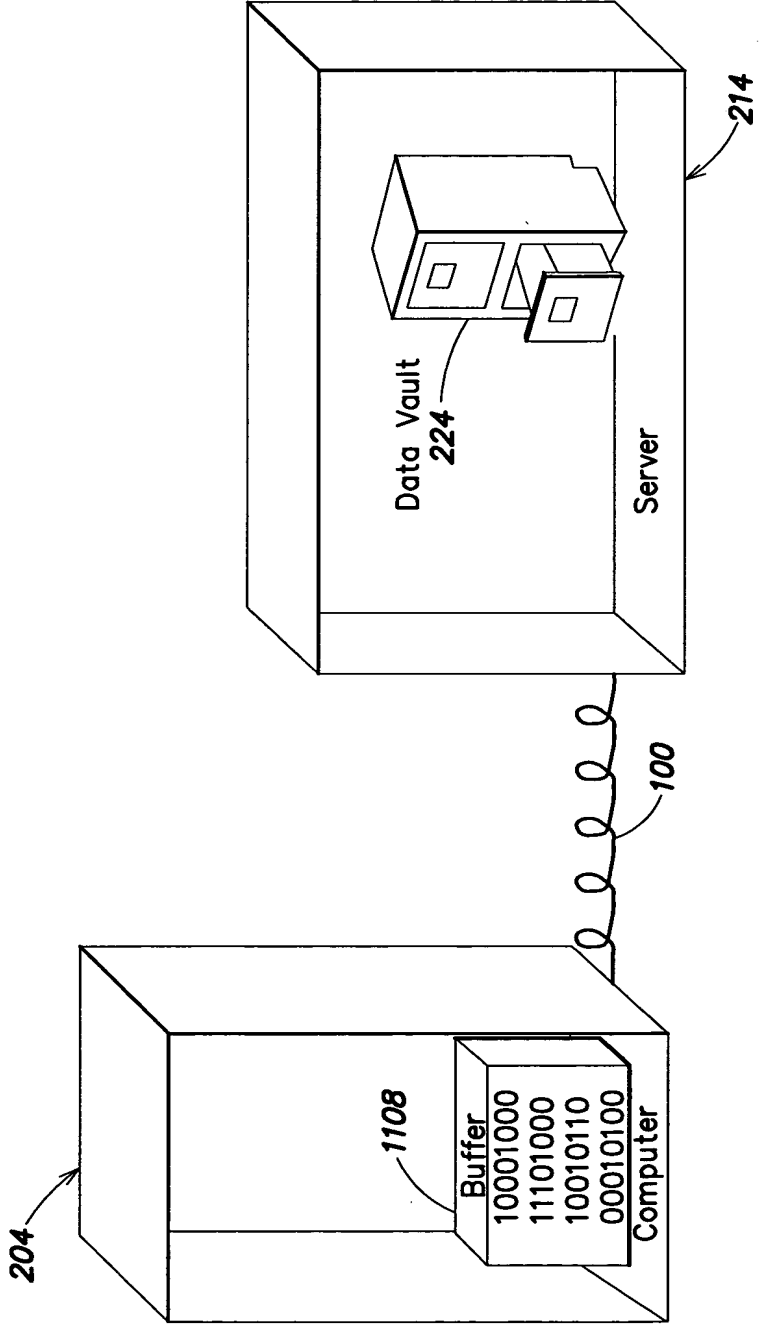


FIG. 13

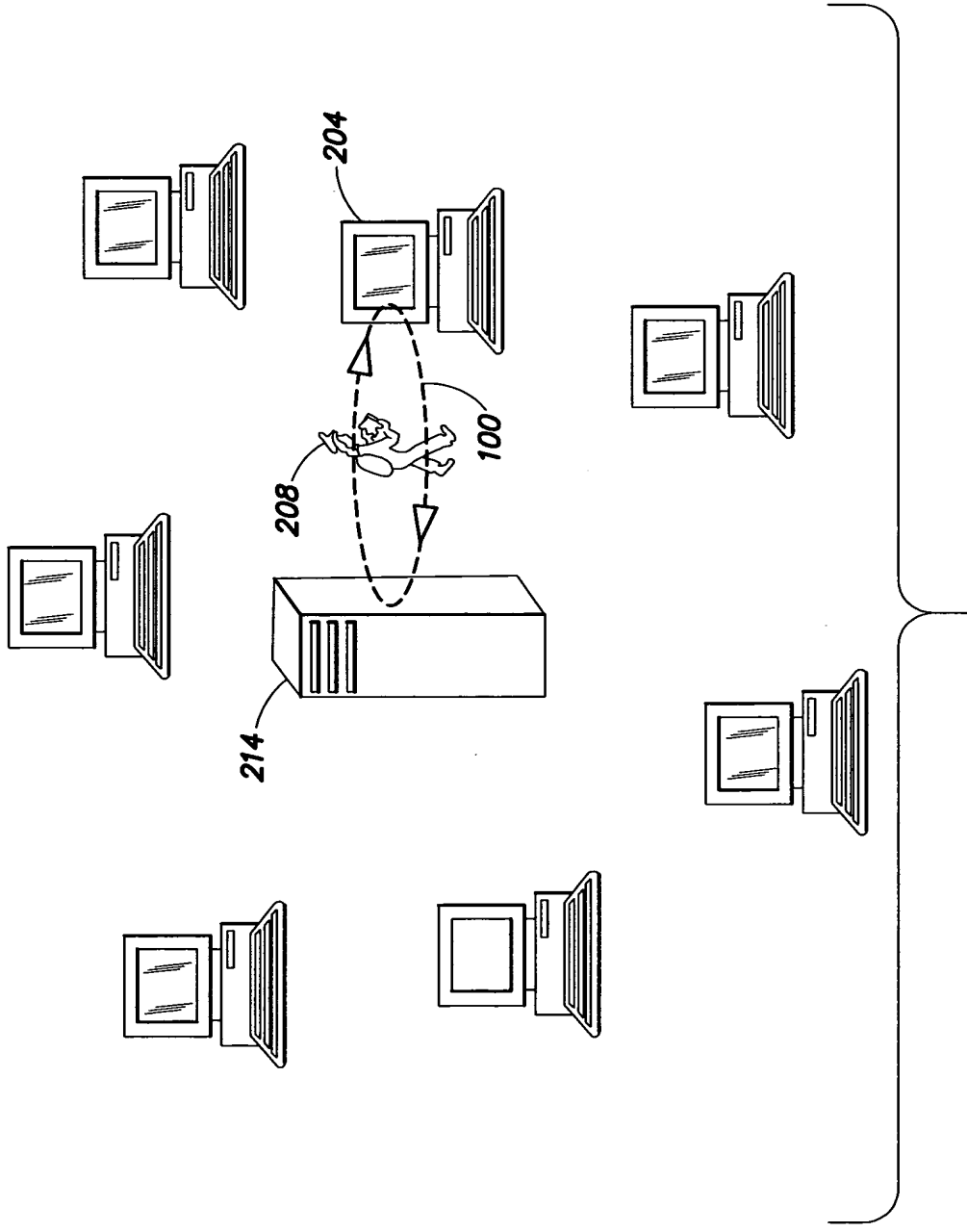


FIG. 14

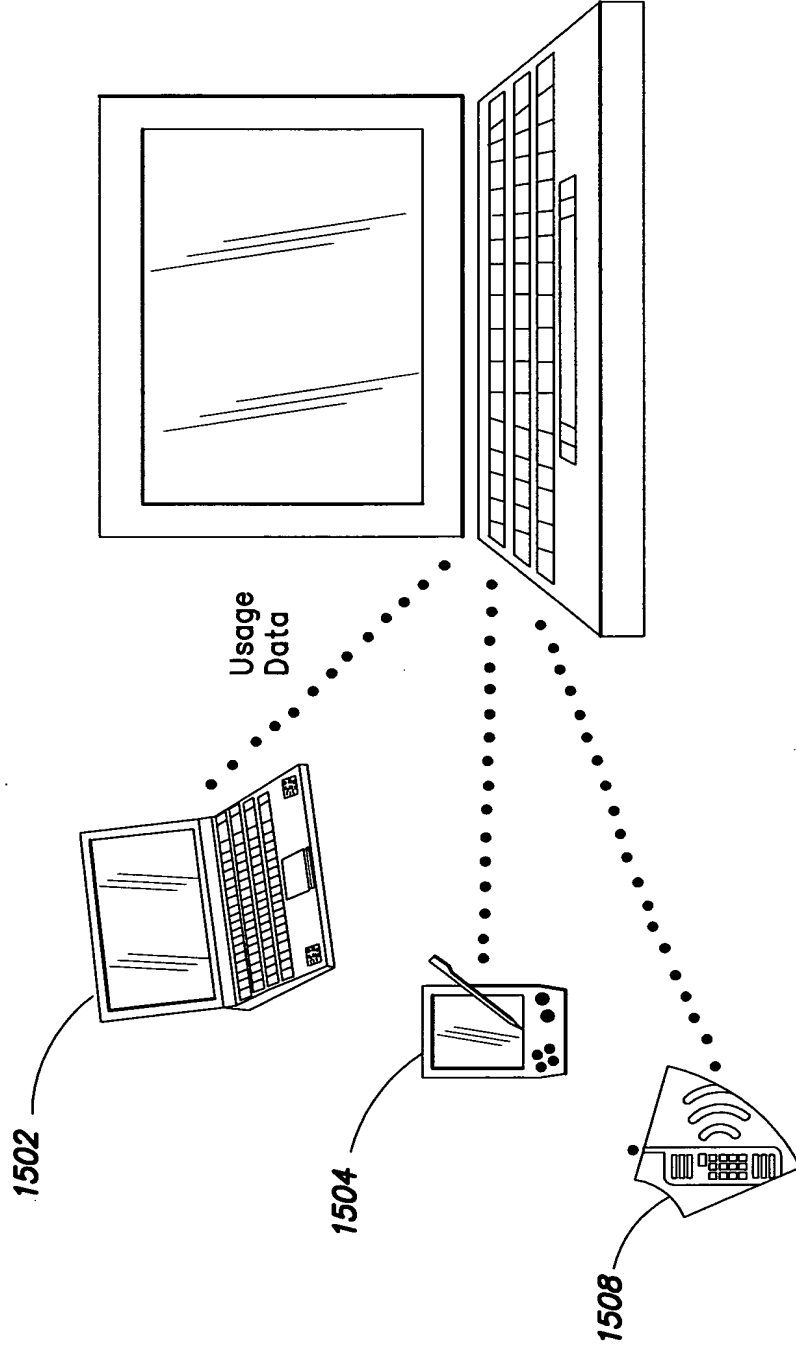


FIG. 15

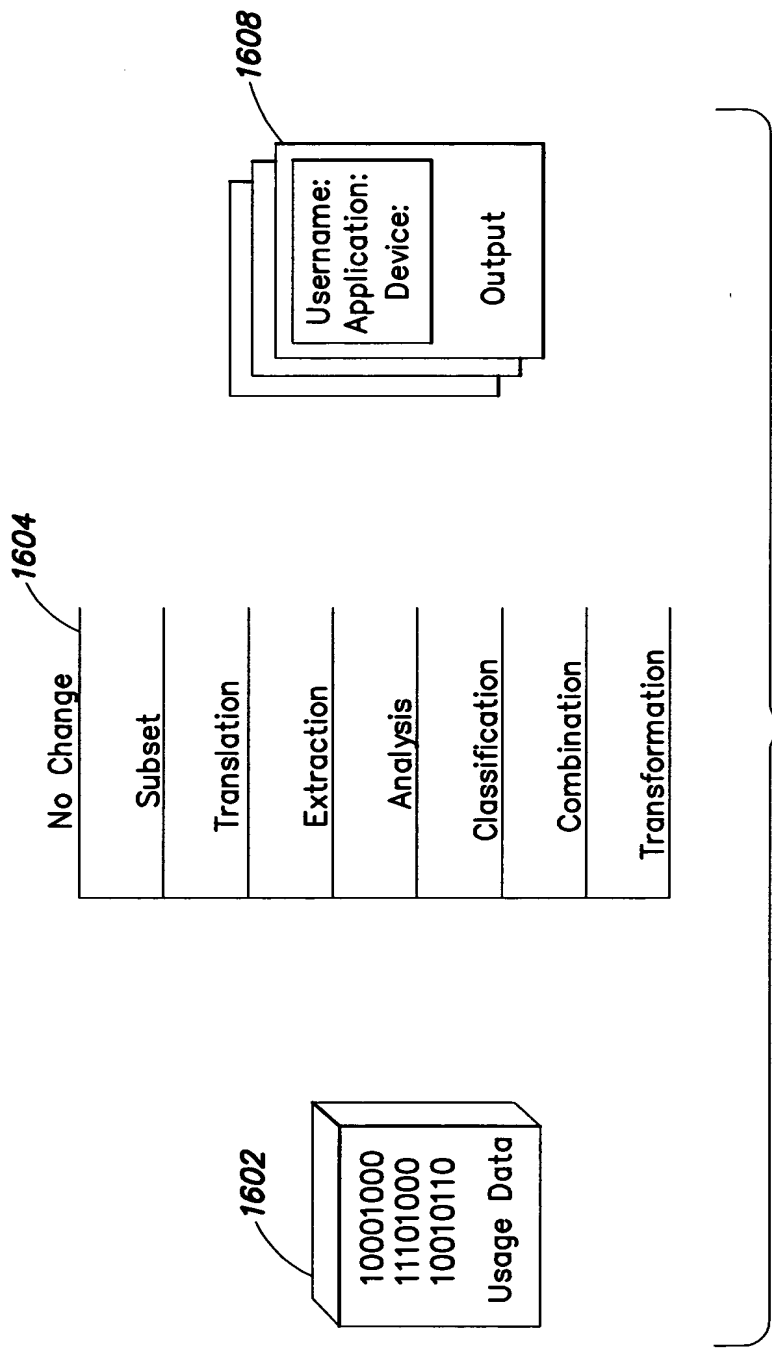


FIG. 16

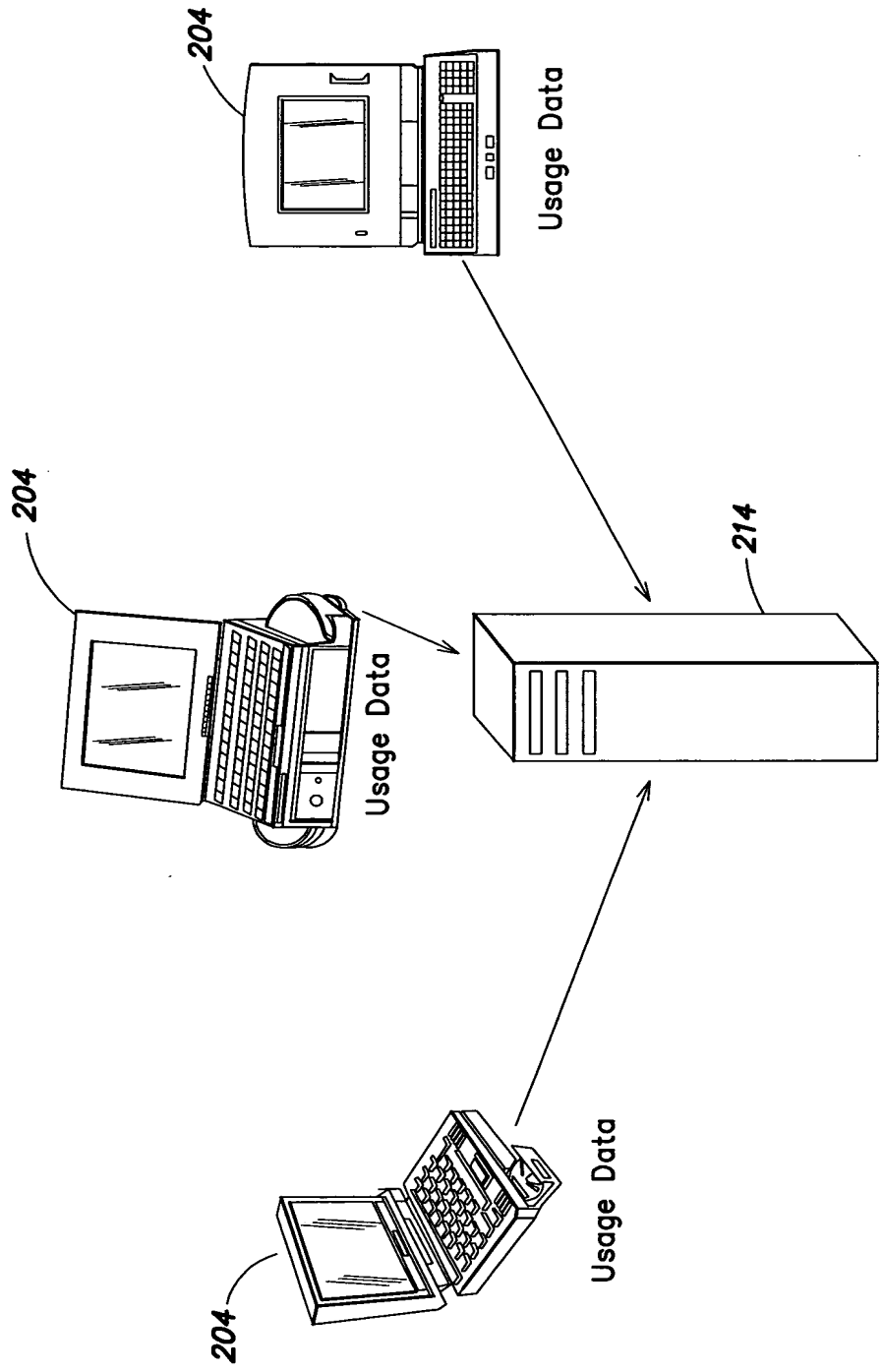


FIG. 17

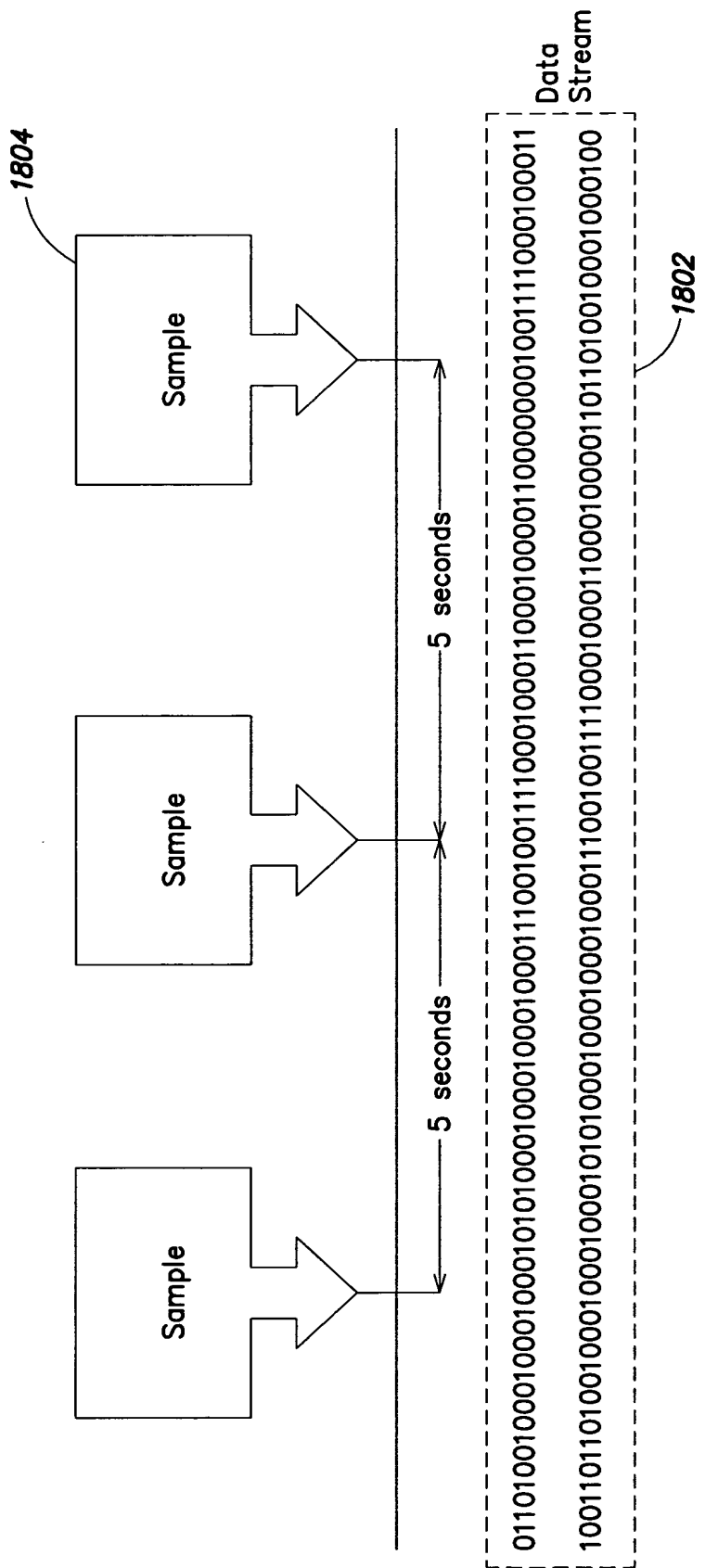


FIG. 18

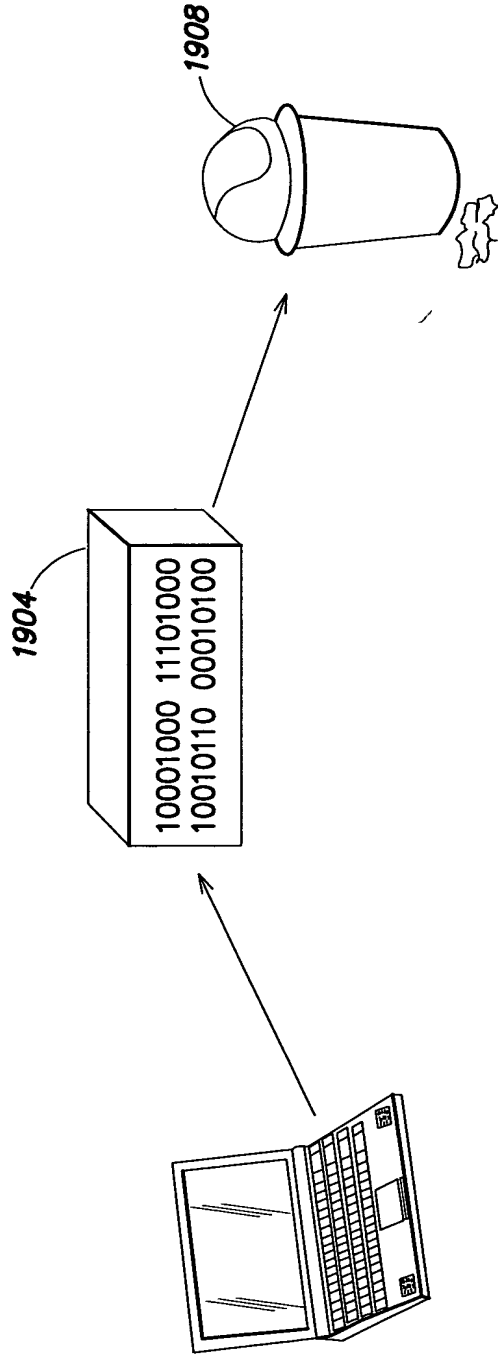


FIG. 19

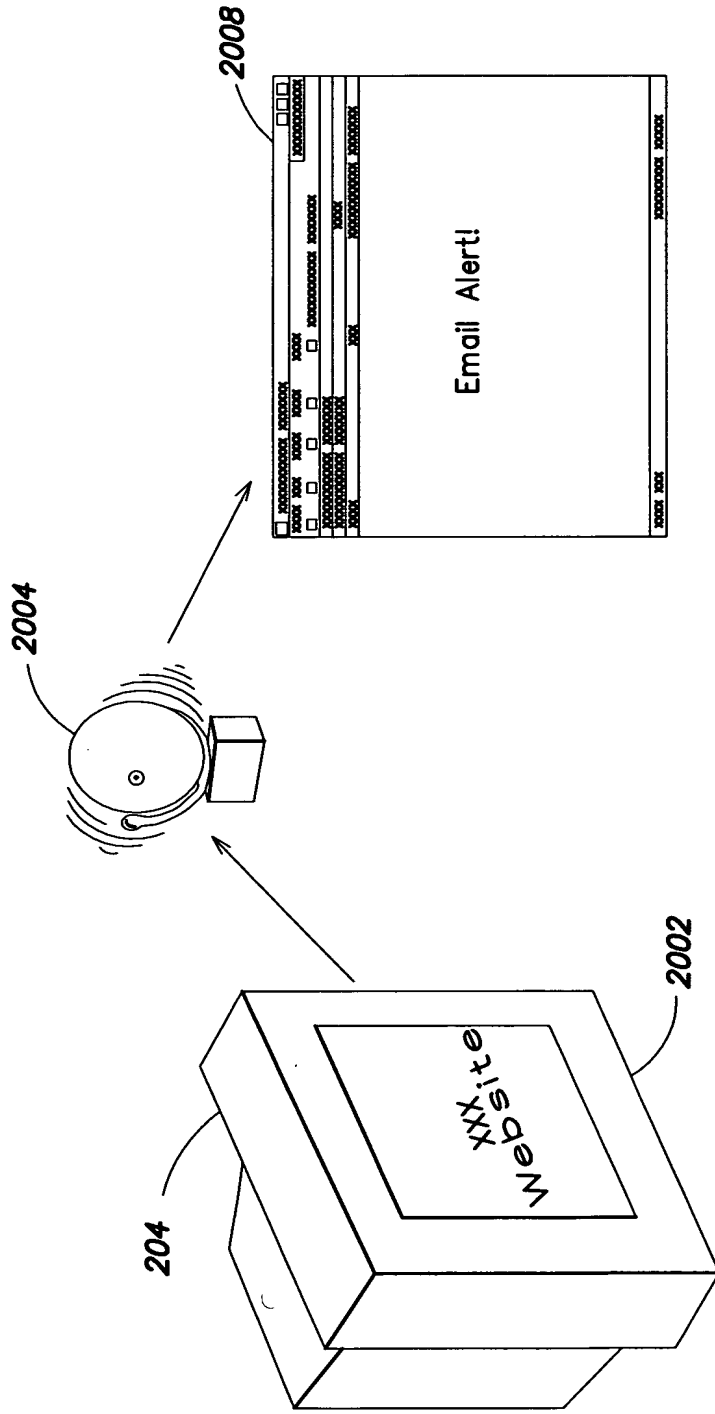


FIG. 20

Sergeant Laboratories - Microsoft Internet Explorer

File Edit View Favorites Tools Help @Send

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Messenger

Address <https://66.112.115.97/cgi-bin/general/main.plx> Go Links

History X
View >>
 3...
 2...
 To...

DataVault Main Page Demo System
Welcome to Aristotle
11/24/2003 1:33P.M.

Event Key

○ = NO Event ○ = Event Emailed
 ⊗ = Event Disabled ⊗ = Event Viewed
 ⊙ = Event Occurred

2100

Utilization

- Computers
- Users
- Applications
- Departments
- General Usage

2102

SECURITY EVENTS

- 2112 System File Change
- 2114 System Directory Creation
- 2118 Application Install/Setup
- 2120 New User(s) Added to System
- 2122 Inactive User(s)
- 2124 Detection of a File Download
- 2128 NT/2K Event Log Status

2106

- 2130 Agent Status-(Pause,Stop,Removed)
- 2132 Backdoor Activity Detection
- 2134 Known Exploit Port Activity
- 2138 New Computer(s) Added to System
- 2140 Inactive Computer(s)
- 2142 Packet Sniffer Detection
- 2144 Modem Usage/Network Properties

2110

Drilldown

- Computers
- Users
- Applications
- Security Events
- Policy Events
- Internet

2108

POLICY EVENTS - 2104

- 2148 Use of an Inappropriate Program
- 2150 Use of a Windows Registry/Policy Editor Program
- 2152 Abnormal Desktop Time Detection
- 2154 Status of the Enterprise Logon and Logoff Policy
- 2158 Detection of a Unregistered User(s) from the Logon Server
- 2160 Detection of Inappropriate Content
- 2162 Internet Time Usage Policy
- 2164 Concurrent Application Licensing Status

Forensic Audit Data

- Computers
- Users
- Archived Data

14 Days x 24 Hrs Computer Activity

Legend
 ⊠ 1%-40%
 ⊡ 40%-60%

11PM
10PM

Internet

Start [Icons] 1:33PM

FIG. 21

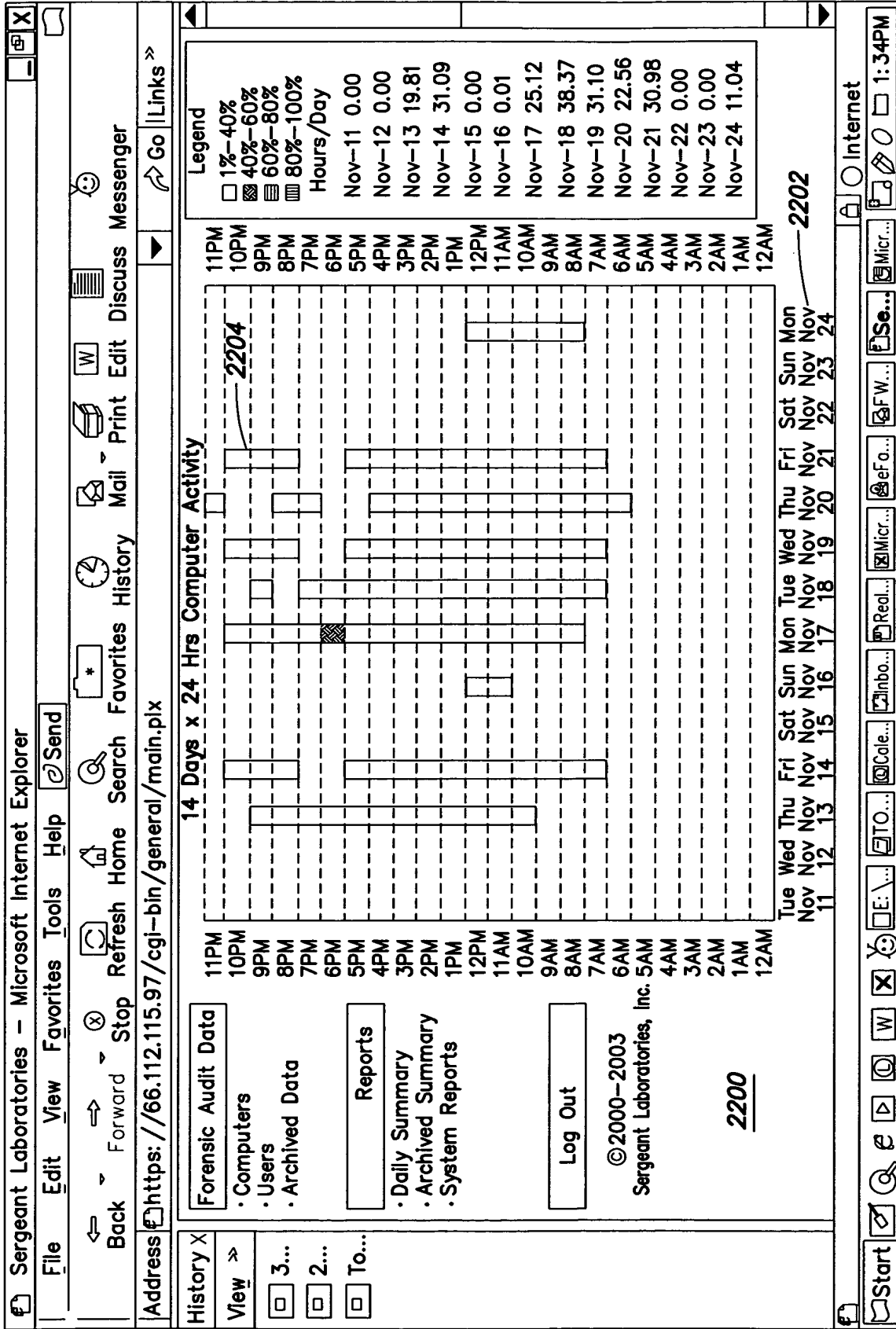


FIG. 22

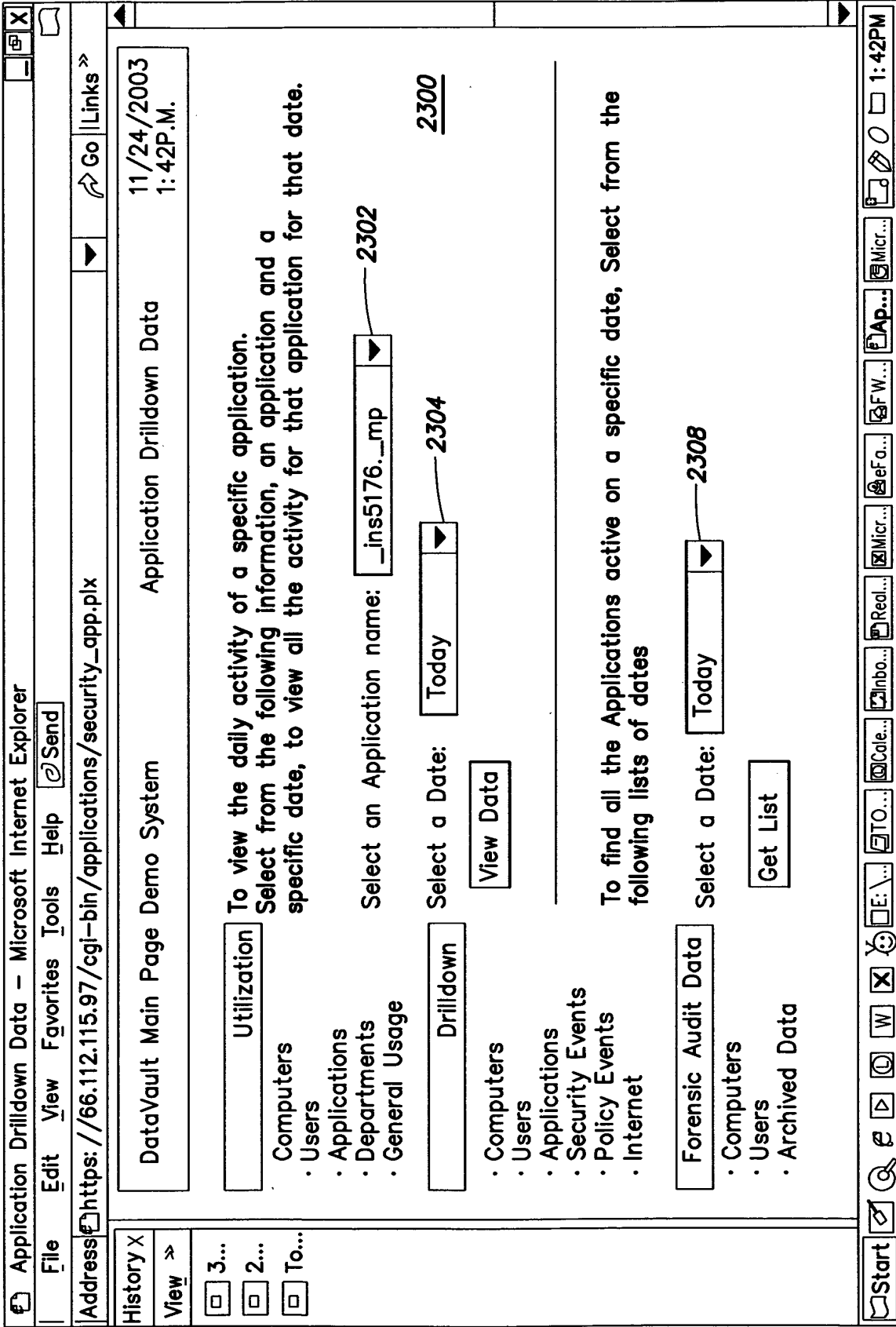


FIG. 23

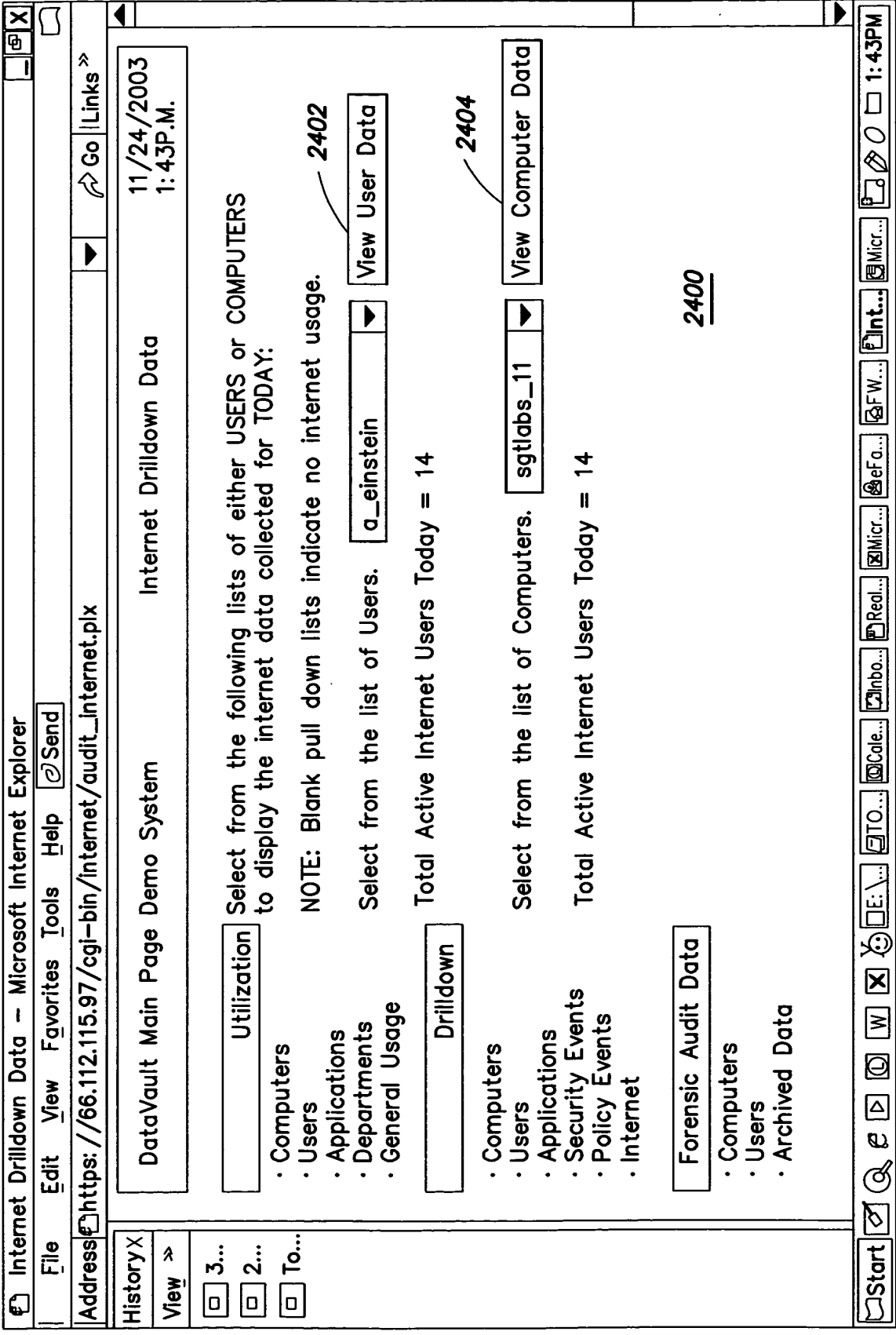


FIG. 24

Internet Drilldown Data - Microsoft Internet Explorer

File Edit View Favorites Tools Help Send

Address: https://66.112.115.97/cgi-bin/internet/audit/internet.plx

Go Links

11/24/2003 1:43 P.M.

DataVault Main Page Demo System Internet Drilldown Data

Internet Activity for Computername: sgtlabs_11

Start	Stop	Total	User	Website Title
10:29:22	10:29:22	0:08 Min	r_jogan	Lincoln Middle School -
10:29:27	10:29:57	0:17 Min	r_jogan	Lincoln Middle School - LMC -
10:30:07	10:30:07	0:08 Min	r_jogan	WebQuest About Volcanoes-by: Louise Jaskoski
10:30:13	10:42:19	0:42 Min	r_jogan	Monitoring Active Volcanoes: Introduction -

2502

2504

2508

Total Internet Time = 0.75 Minutes

2500

Utilization

- Computers
- Users
- Applications
- Departments
- General Usage

Drilldown

- Computers
- Users
- Applications
- Security Events
- Policy Events
- Internet

Forensic Audit Data

- Computers
- Users
- Archived Data

History X

View >>

3...
2...
To...

Start

Start

End

Print

Refresh

Home

Back

Forward

Stop

Search

Tools

Micro...

Int...

FW...

Def a...

Micr...

Micr...

Real...

Inbo...

Cal...

TO...

E:...

W

X

W

1:43PM

FIG. 25

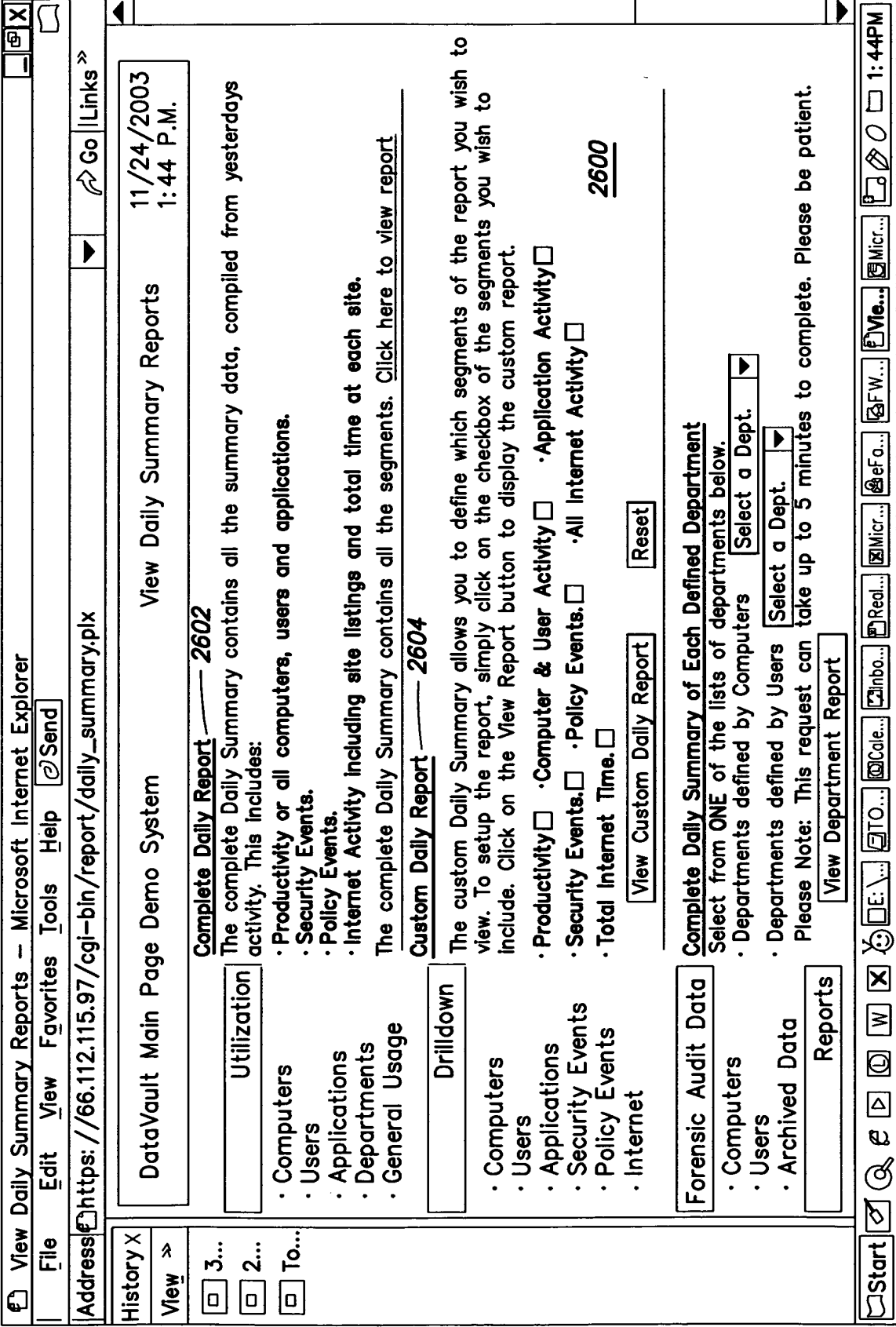


FIG. 26

View Daily Summary Reports - Microsoft Internet Explorer

File Edit View Favorites Tools Help Send

Address https://66.112.115.97/cgi-bin/report/daily_summary.pix Go Links >

History X
View >>

3...
 2...
 To...

· Policy Events
· Internet

Complete Daily Summary of Each Defined Department — 2702
Select from ONE of the lists of departments below.

- Departments defined by Computers ▾
- Departments defined by Users ▾

Please Note: This request can take up to 5 minutes to complete. Please be patient.

Custom Daily Summary of Each Defined Department — 2704
Select from ONE of the lists of departments below.

- Departments defined by Computers ▾
- Departments defined by Users ▾

The custom Department Summary allows you to define which segments of the report you wish to view. To setup the report, simply click on the checkbox of the segments you wish to include. Click on the View Report button to display the custom report.

- Productivity · Computer & User Activity · Application Activity — 2710
- Security Events · Policy Events · All Internet Activity — 2718
- Total Internet Time — 2714
- Total Internet Time — 2720

Please Note: This request can take up to 5 minutes to complete. Please be patient.

©2000-2003
Sergeant Laboratories, Inc.

Start Search Home W X E... TO... Cale... Inbo... Real... Micr... Def a... F W... View... Micr... 1:44PM

FIG. 27

5thColumn DataVault: Daily Report for - 11-23-2003 - Microsoft Internet Explorer

File Edit View Favorites Tools Help @Send

Address: https://66.112.115.97/report/report.html

Go Links

History X

View >>

3...

2...

To...

5thColumn DataVault: Daily Report
11-23-2003

SUMMARY

<u>SECURITY EVENTS</u>	<u>COMPUTERS</u>	<u>POLICY EVENTS</u>	<u>APPLICATIONS</u>
	<u>USERS</u>	<u>INTERNET EVENTS</u>	<u>Main Page</u>
	<u>2820</u>	<u>2822</u> <u>2828</u>	<u>2802</u>

Overall Enterprise Activity

Total Active Computers:	0	Total Agent Computers:	31	Pct. Used:	0.000%
Total Active Users:	0	Total Agent Users:	31	Pct. Used:	0.000%
Total Active Apps:	0	Total Agent Apps:	134	Pct. Used:	0.000%
Usage Hrs.:	<u>2824</u> 0.00	Pct. Used(24Hr):	0.000%	Pct. Used(8Hr):	0.000%

Computer and User Activity

<u>Computer Name</u>	<u>Hrs</u>	<u>Users</u>	<u>Computer Name</u>	<u>Hrs</u>	<u>Users</u>
<u>User Name</u>	<u>Hrs</u>	<u>Computers</u>	<u>User Name</u>	<u>Hrs</u>	<u>Computers</u>

Application Activity - (Red denotes new application)

<u>EXE Name</u>	<u>Hrs</u>	<u>Computers</u>	<u>EXE Name</u>	<u>Hrs</u>	<u>Computers</u>

Security Events

Policy Events

Complete Internet Data

(c) Copyright 2001-2002 Sergeant Laboratories, Inc.

Start [Icons] 1:45PM

FIG. 28

Computer Drilldown Data - Microsoft Internet Explorer

File Edit View Favorites Tools Help Send

Address: https://66.112.115.97/cgi-bin/computers/security_computers.plx

Go Links

11/24/2003 1:36 P.M.

Computer Drilldown Data

Displaying results for sgtlabs_04 on Fri 11-21-2003

Username	Time	Active Minutes	Application
m_klien	08:00-08:14:59 am	00.25 Min.	Microsoft Word
m_klien	08:15-08:29:59 am	00.50 Min.	Microsoft Word
m_klien	08:15-08:29:59 am	00.08 Min.	agentsvr.exe
m_klien	08:15-08:29:59 am	01.67 Min.	grpwise.exe
m_klien	08:15-08:29:59 am	00.08 Min.	Microsoft Windows Explorer
m_klien	08:15-08:29:59 am	00.42 Min.	sol.exe
m_klien	09:45-09:59:59 am	04.50 Min.	grpwise.exe
m_klien	09:45-09:59:59 am	00.17 Min.	Microsoft Windows Explorer
m_klien	09:45-09:59:59 am	01.83 Min.	sol.exe
m_klien	11:00-11:14:59 am	00.33 Min.	grpwise.exe
m_klien	11:00-11:14:59 am	00.08 Min.	Microsoft Windows Explorer
m_klien	11:00-11:14:59 am	01.08 Min.	sol.exe
m_klien	11:15-11:29:59 am	13.75 Min.	sol.exe
m_klien	11:15-11:29:59 am	00.08 Min.	grpwise.exe
m_klien	11:15-11:29:59 am	00.08 Min.	Microsoft Windows Explorer
m_klien	11:30-11:44:59 am	12.50 Min.	sol.exe
m_klien	11:30-11:44:59 am	00.08 Min.	grpwise.exe
m_klien	12:00-12:14:59 pm	00.08 Min.	Microsoft Windows Explorer
m_klien	12:00-12:14:59 pm	06.00 Min.	sol.exe
m_klien	12:00-12:14:59 pm	00.08 Min.	grpwise.exe
m_klien	12:15-12:29:59 pm	14.25 Min.	sol.exe

Utilization

- Computers
- Users
- Applications
- Departments
- General Usage

Drilldown

- Computers
- Users
- Applications
- Security Events
- Policy Events
- Internet

Forensic Audit Data

- Computers
- Users
- Archived Data

History X

View >>

3... 2... To...

Start Search Home W X E TO... Cal... Inbo... Real... Micr... Def.a... F.W... Co... Micr... 1:36PM

FIG. 29

Application Utilization Data - Microsoft Internet Explorer

File Edit View Favorites Tools Help @Send

Address: https://66.112.115.97/cgi-bin/applications/app_dd.plx

History X
View >>

3...
 2...
 To...

DataVault Main Page Demo System

Select from the list of Applications to view 14 days worth of usage.

Application Utilization Data

11/24/2003
1:37 P.M.

Sort A-Z Current Usage Statistics

Application: acror32.exe

Microsoft Word 22.74
Microsoft Internet Explorer 8.23
arpwise.exe 19.68
Microsoft PowerPoint 5.80
sol.exe 12.70
mtg.exe 16.67
Microsoft Windows Explorer 1.77
ntvdm.exe 15.55
mispub.exe 9.54
pcsws.exe 19.88
pinball.exe 2.67
Microsoft Excel Spreadsheet 3.49
artgalry.exe 76
pcat32t.exe 20
winmine.exe 18
pratica.musica.exe 19
agentsvr.exe 92
mworks.exe 2
cica32t.exe 1
mispaint.exe 15
wordpad.exe 5
wmpayer.exe 23
freecell.exe 11
msimn.exe 8
clworks.exe 3
sndrec32.exe 12
rundll32.exe 19
signlab5.exe 2
sibelius.exe 1
addressbook.exe 6

Usage Time: 3000

3000

2914

3004

Drilldown

Utilization

Computers
Users
Applications
Departments
General Usage

Forensic Audit Data

Computers
Users
Archived Data

Start Search Home W X Print Mail Micr... Ap... FW... Ef... Micr... Red... Inbo... Cate... TO... E... Start

1:37PM

FIG. 30

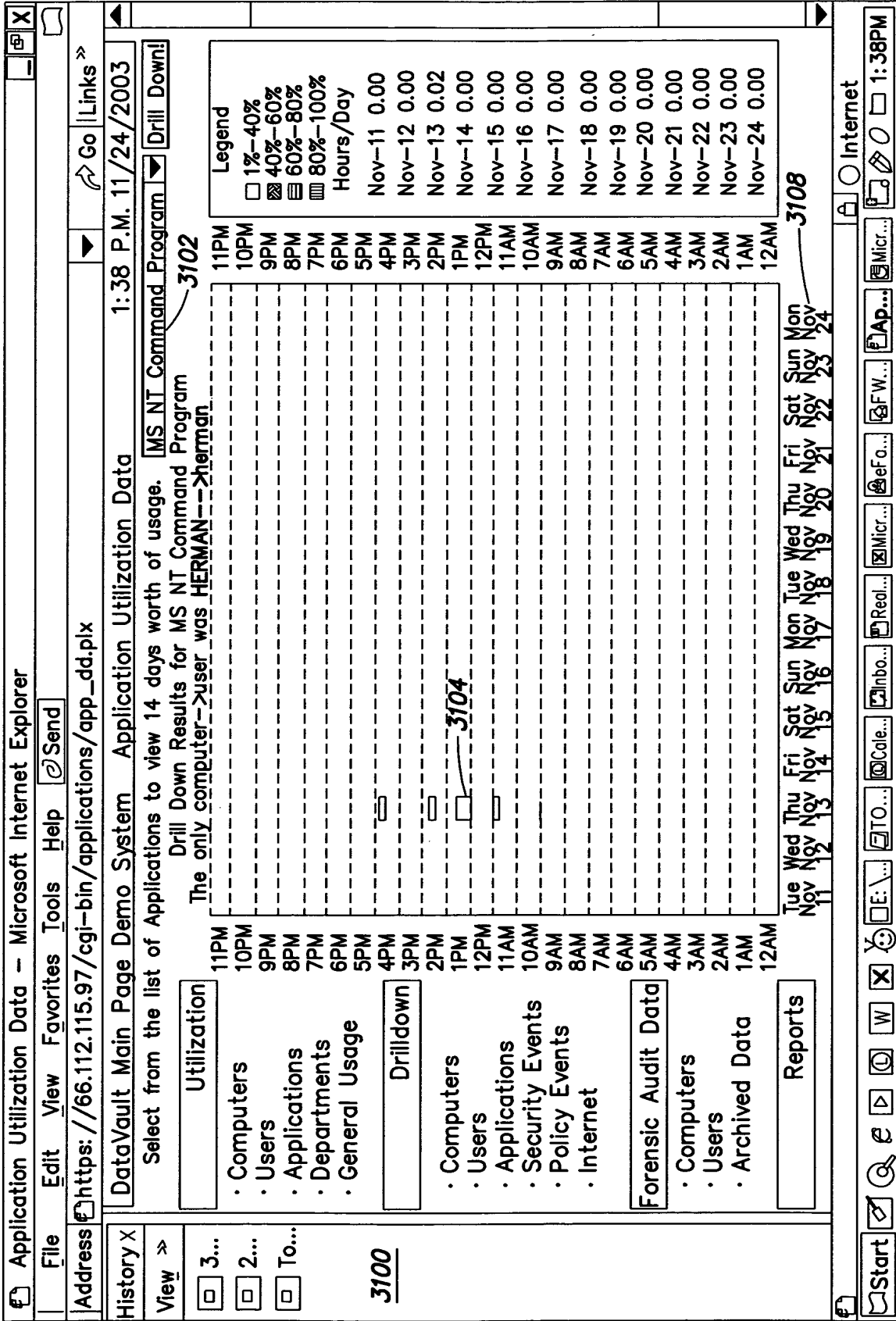


FIG. 31

Dept. Utilization Data - Microsoft Internet Explorer

File Edit View Favorites Tools Help Send

Address: https://66.112.115.97/cgi-bin/department/dept_dd.plx

Go Links >

11/24/2003 1:39P.M.

DataVault Main Page Demo System Dept. Utilization Data Administration

Select from the list of computers to view 14 days worth of usage.

Current Usage Statistics of ALL 9 Active Departments. Drill Down

Department Name	Dept. Computers			Dept. Users					
	Qty.	Time	Avg.	Qty.	Time	Avg.			
Administration	6	832.42	138.74	0	0	0.00			
Department_01	0	0	0.00	8	994.37	124.30			
Department_03	0	0	0.00	23	2700.69	117.42			
Department_08	24	2844.39	118.52	0	0	0.00			
MPCDept	0	0	0.00	0	0	0.00			
Resource_Center	0	0	0.00	0	0	0.00			
Student	1	18.15	18.15	0	0	0.00			
StudentComputers	0	0	0.00	0	0	0.00			
Test_Dept_02	0	0	0.00	0	0	0.00			
				3202	3204	3208	3212	3214	3218

Utilization

- Computers 3220
- Users 3222
- Applications
- Departments
- General Usage

Drilldown

- Computers
- Users
- Applications
- Security Events
- Policy Events
- Internet

Forensic Audit Data

- Computers
- Users
- Archived Data

3200

Start Search Home W X E: \ TO... Cal... Inbo... Real... Micr... Def a... FW... De... Micr... 1:39PM

FIG. 32

General Utilization Data - Microsoft Internet Explorer

File Edit View Favorites Tools Help Send

Address: https://66.112.115.97/cgi-bin/general/gen_stats.plx Go Links >>

11/24/2003 1:39 P.M.

DataVault Main Page Demo System **General Utilization Data**

Daily Computer/User Usage

Users/Comps

12 11 10 9 8 7 6 5 4 3 2 1

12123456789101112134567891011

Current Number of Users = 13 @ 12:24
Current Number of Computers = 13 @ 12:24

Productivity of all Computers

Usage %

100 90 80 70 60 50 40 30 20 10 0

12123456789101112134567891011

Current System Usage % = .06% @ 12:24

Utilization — 3220

- Computers — 3308
- Users
- Applications
- Departments
- General Usage

Drilldown

- Computers
- Users
- Applications
- Security Events
- Policy Events
- Internet

Forensic Audit Data

- Computers
- Users
- Archived Data

Reports

3300

Start Search Home W X E: \ TO... Cale... Inbo... Real... Micr... Ge... F.W... Micr... 1:40PM

FIG. 33

Policy Event Data - Microsoft Internet Explorer

File Edit View Favorites Tools Help Send

Address: https://66.112.115.97/cgi-bin/policy/security_policy.plix

Go Links >

11/24/2003 1:40 P.M.

DataVault Main Page Demo System Policy Event Data

Listing of Todays Policy Events (Gray = New Event) 3404 3408

3402 Mon Nov 24 at 12:00:03 User: d_jones Computer: sgtlabs_02
 Use of an Inappropriate Program - sol.exe

3412 Mon Nov 24 at 11:04:02 User: j_kennedy Computer: sgtlabs_28
 Use of an Inappropriate Program - sol.exe

2914 Mon Nov 24 at 11:03:03 User: j_kennedy Computer: sgtlabs_28
 Use of an Inappropriate Program - sol.exe

Mon Nov 24 at 11:02:03 User: j_kennedy Computer: sgtlabs_28
 Use of an Inappropriate Program - sol.exe

Mon Nov 24 at 11:01:04 User: j_kennedy Computer: sgtlabs_28
 Use of an Inappropriate Program - sol.exe

Mon Nov 24 at 10:59:01 User: j_kennedy Computer: sgtlabs_28
 Use of an Inappropriate Program - sol.exe

Mon Nov 24 at 10:57:04 User: j_kennedy Computer: sgtlabs_28
 Use of an Inappropriate Program - sol.exe

Mon Nov 24 at 10:55:10 User: j_kennedy Computer: sgtlabs_28
 Use of an Inappropriate Program - so.exe

Mon Nov 24 at 10:51:00 User: l_charlie Computer: sgtlabs_10
 Use of an Inappropriate Program - sol.exe

Mon Nov 24 at 10:50:04 User: l_charlie Computer: sgtlabs_10
 Use of an Inappropriate Program - sol.exe

Utilization

- Computers
- Users
- Applications
- Departments
- General Usage

Drilldown

- Computers
- Users
- Applications
- Security Events
- Policy Events
- Internet

Forensic Audit Data

- Computers
- Users
- Archived Data

Reports

3400

Start [Navigation icons] 1:41PM

FIG. 34

General Utilization Data - Microsoft Internet Explorer

File Edit View Favorites Tools Help Send

Address: https://66.112.115.97/cgi-bin/general/gen_stats.pix

History X

View >>

3... 2... To...

- Users
- Applications — 3518
- Security Events
- Policy Events
- Internet

- Computers
- Users
- Archived Data

- Daily Summary
- Archived Summary
- Systems Reports

© 2000-2003
Sergeant Laboratories, Inc.

Current Number of Users = 13 @ 12:24
 Current Number of Computers = 13 @ 12:24
 Productivity of all Computers

12123456789101121234567891011

Current System Usage % = .06% @ 12:24

Top Ten Applications Used

Application	Days	Hours	#Users	#Computers
1. Microsoft Word	08	73.84	31	31
2. grpwise.exe	08	34.70	18	18
3. sol.exe	08	18.05	15	15
4. Microsoft Internet Explorer	08	16.37	29	29
5. mspub.exe	07	10.8	16	16
6. ntvdm.exe	08	10.43	13	13
7. Microsoft PowerPoint	08	10.04	13	13
8. mtg.exe	08	09.28	07	07
9. Microsoft Windows Explorer	09	08.01	31	31
10. pcsws.exe	08	05.54	04	04

3502 — 3504 — 3508 — 3512 — 3514

FIG. 35

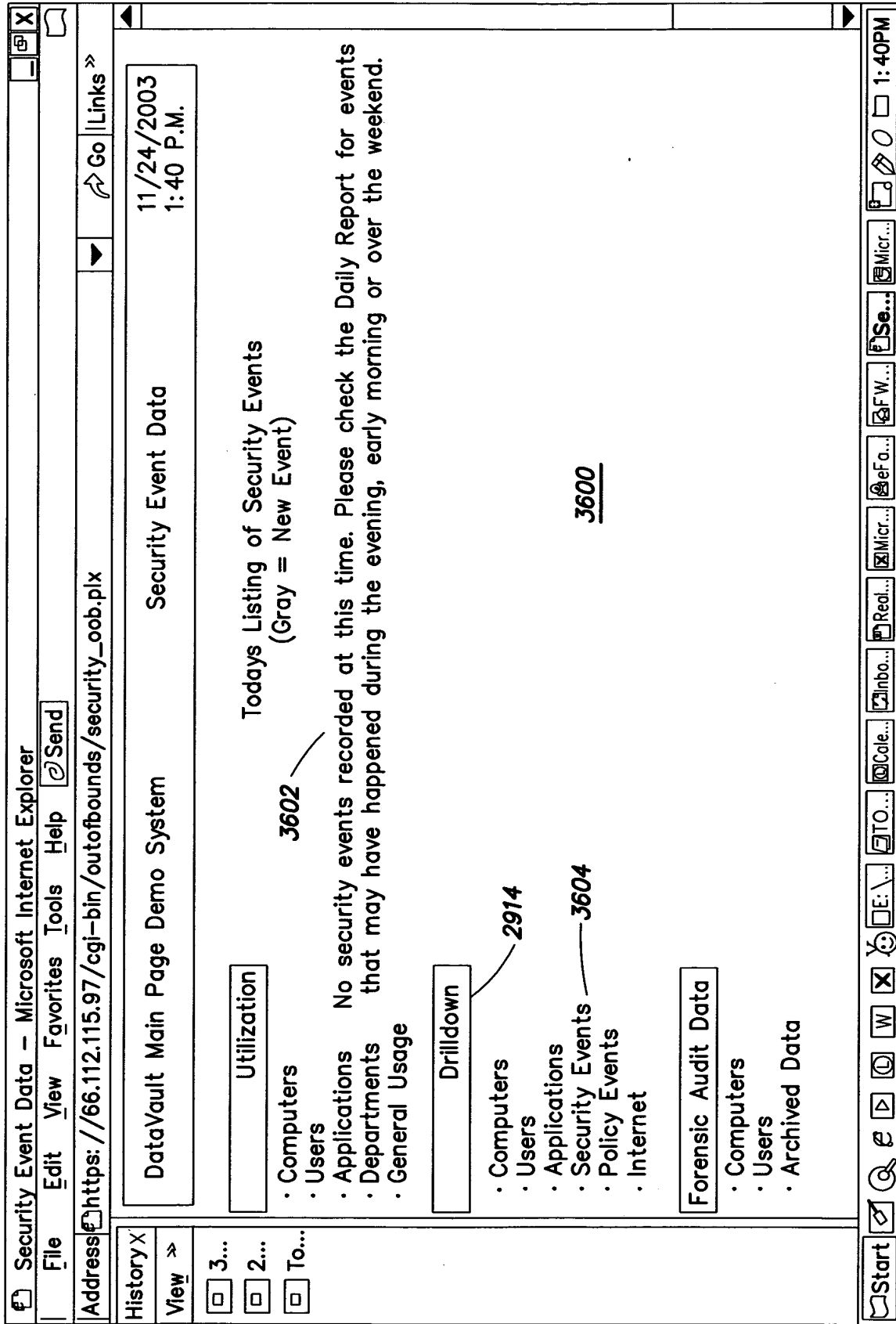


FIG. 36

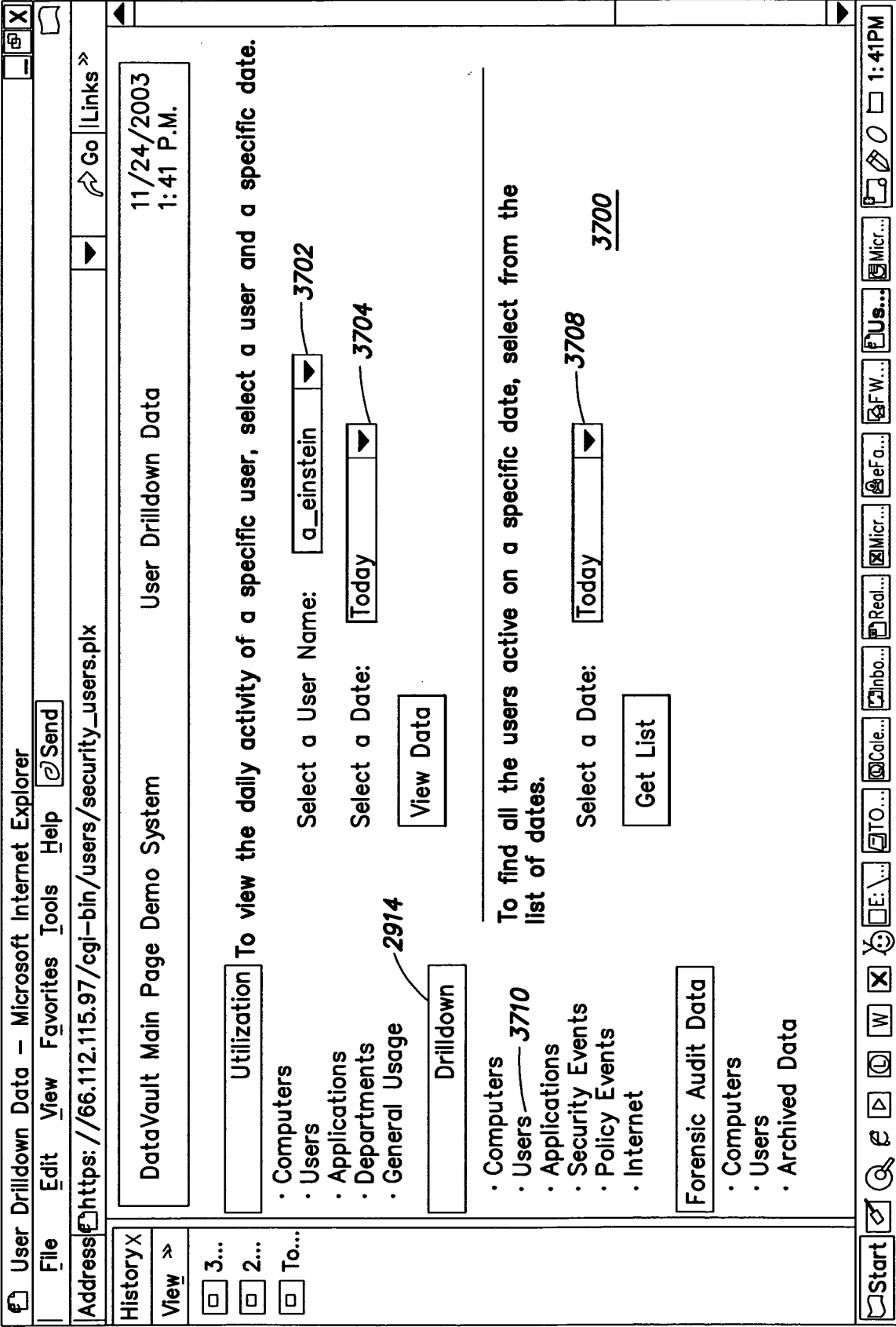


FIG. 37

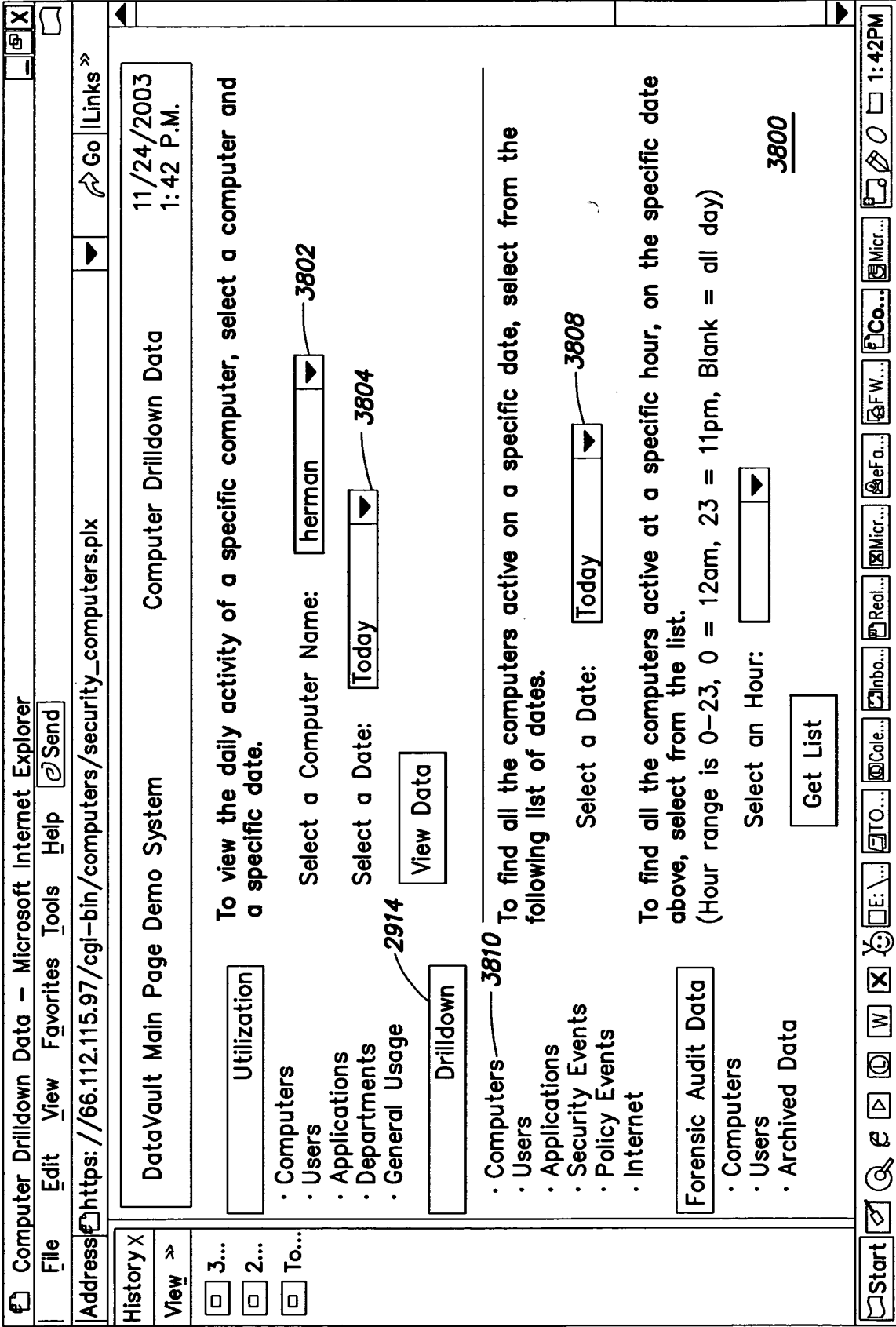


FIG. 38

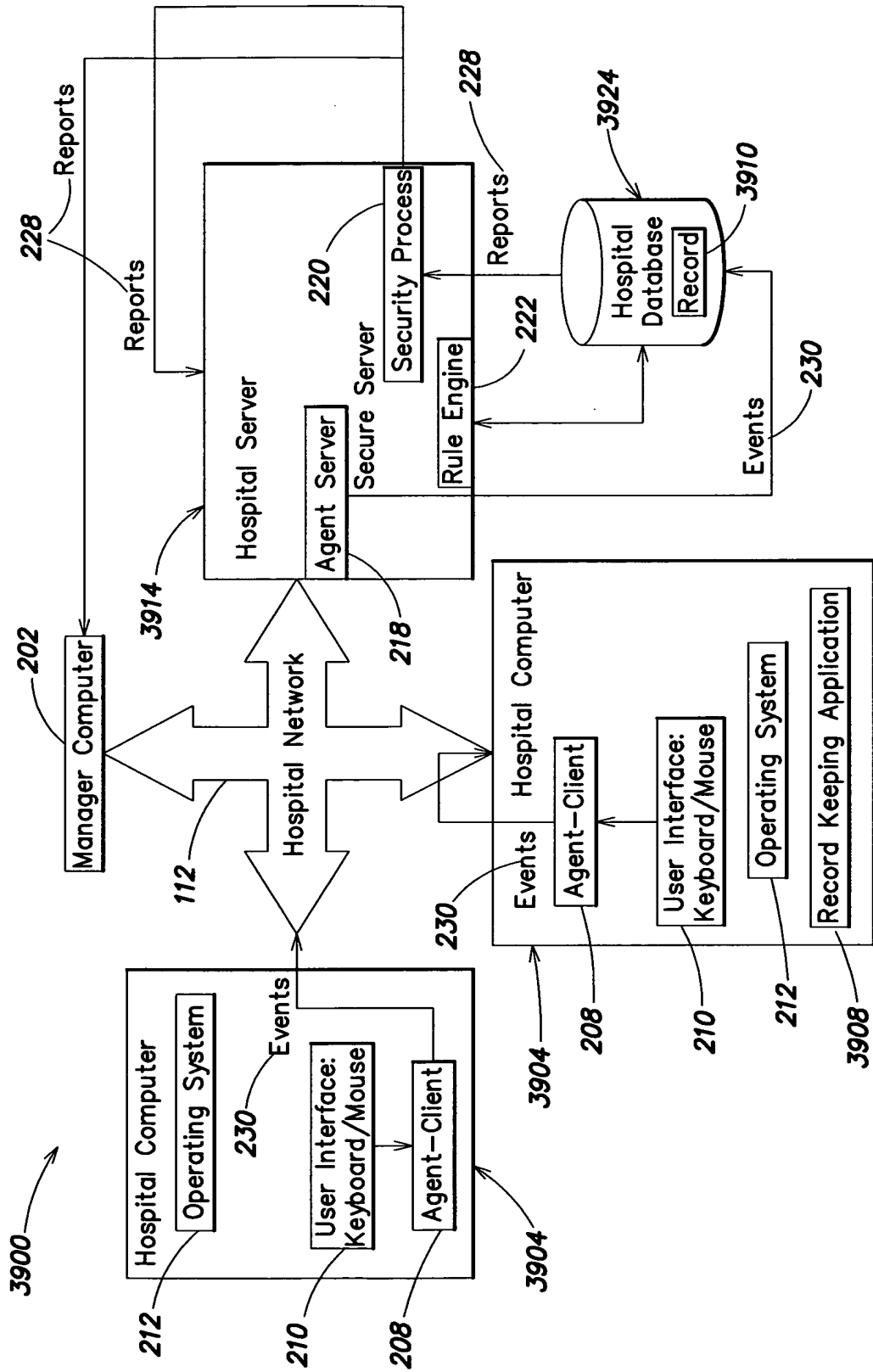


FIG. 39

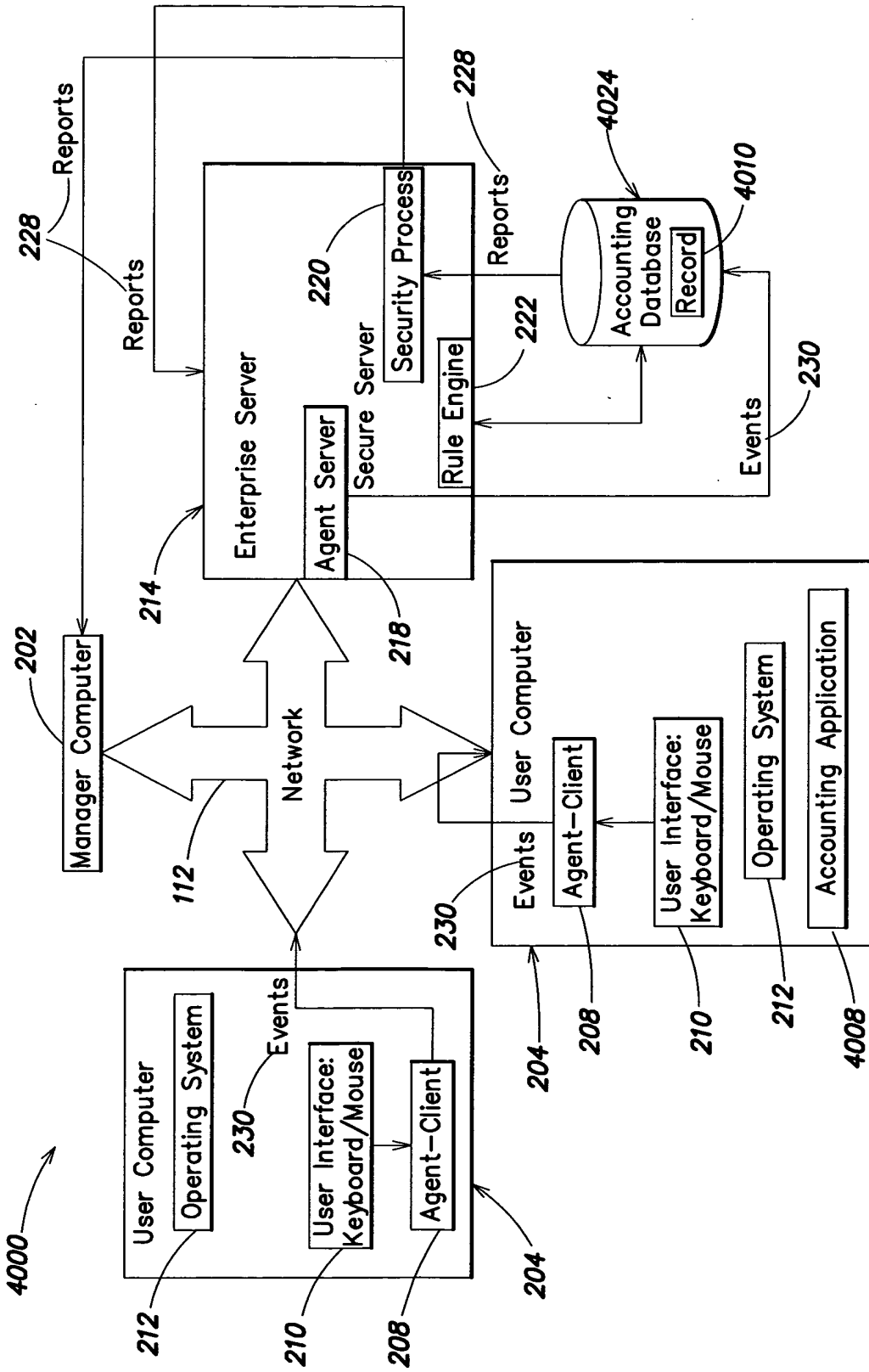


FIG. 40

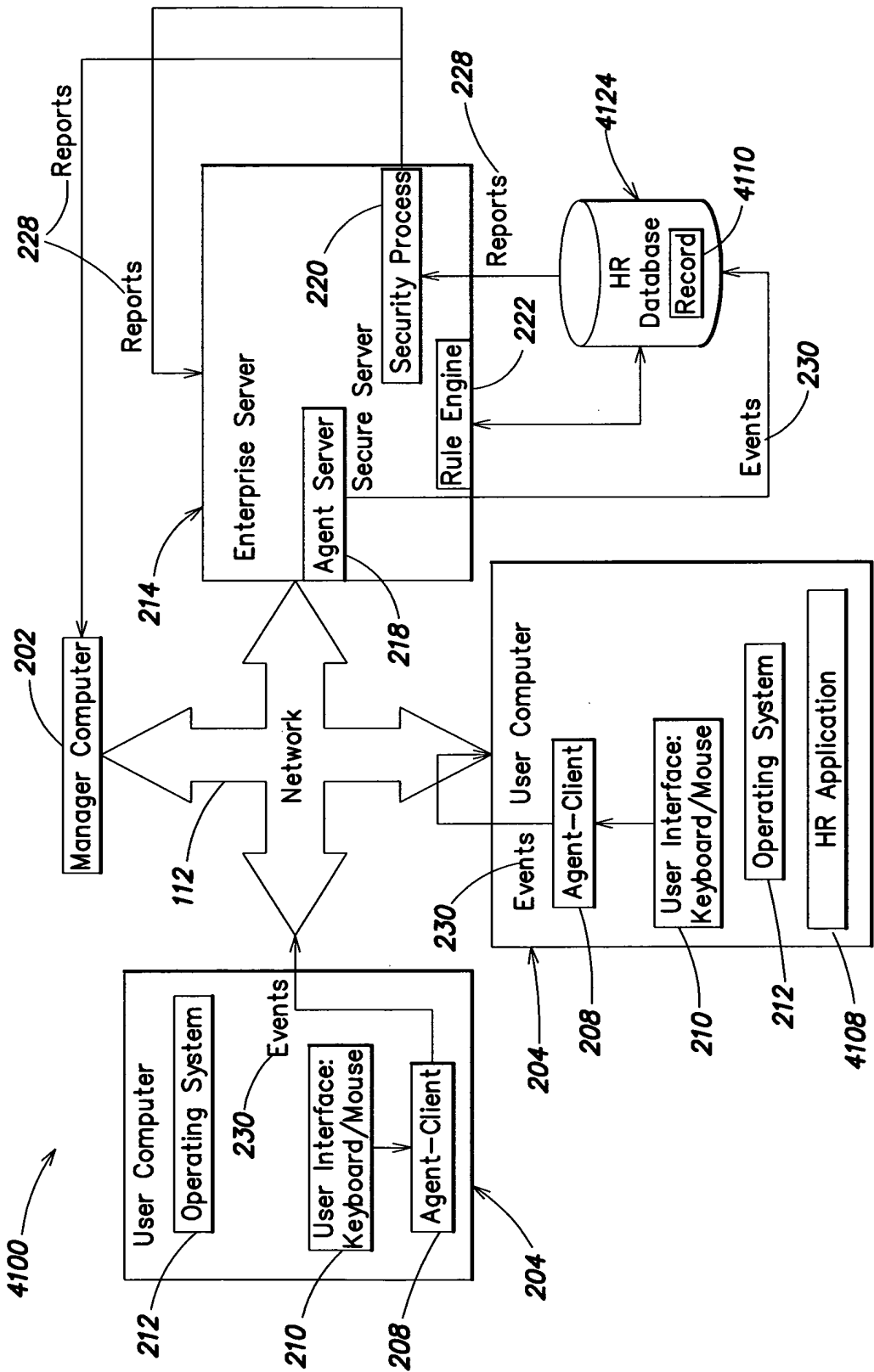


FIG. 41

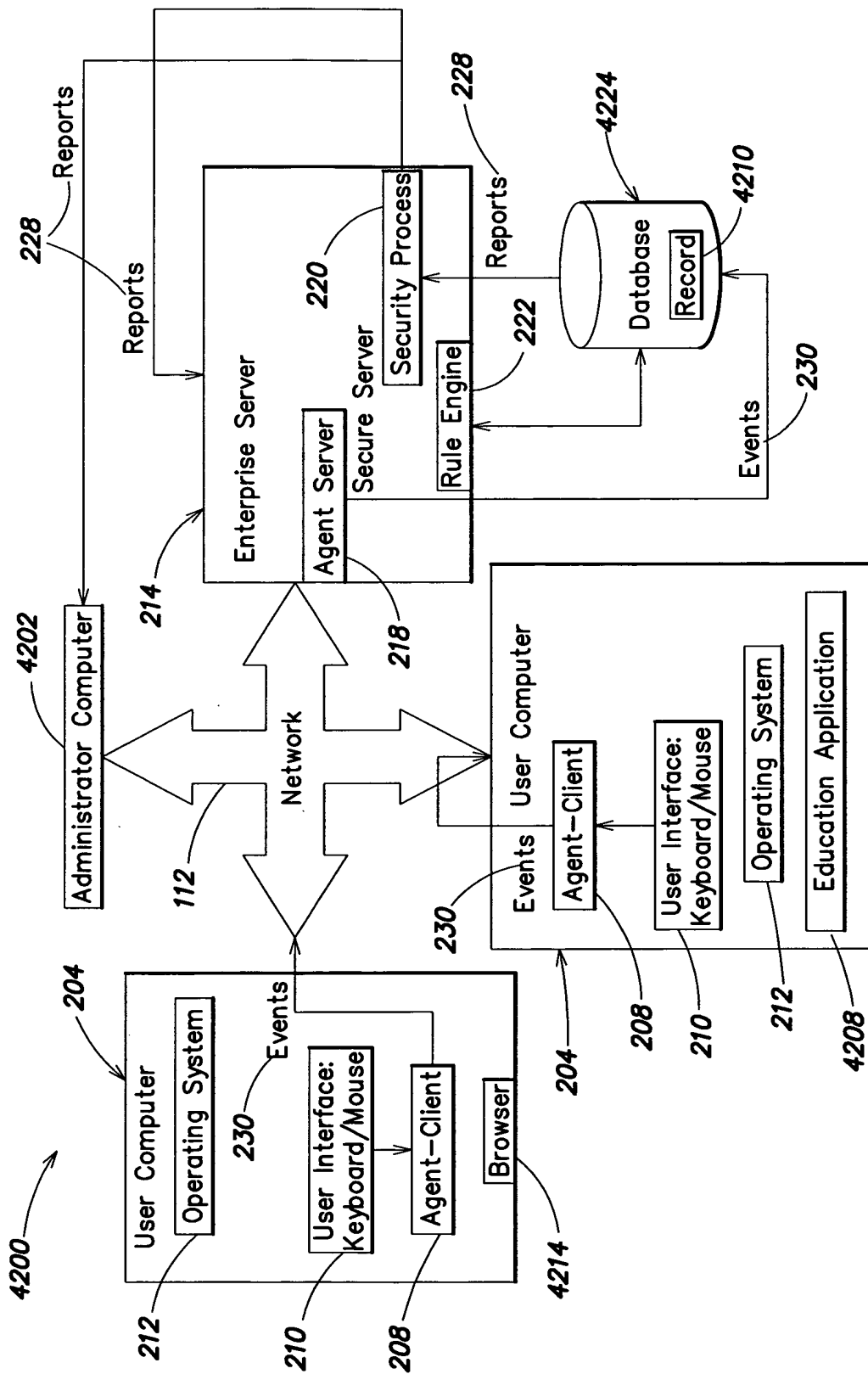


FIG. 42

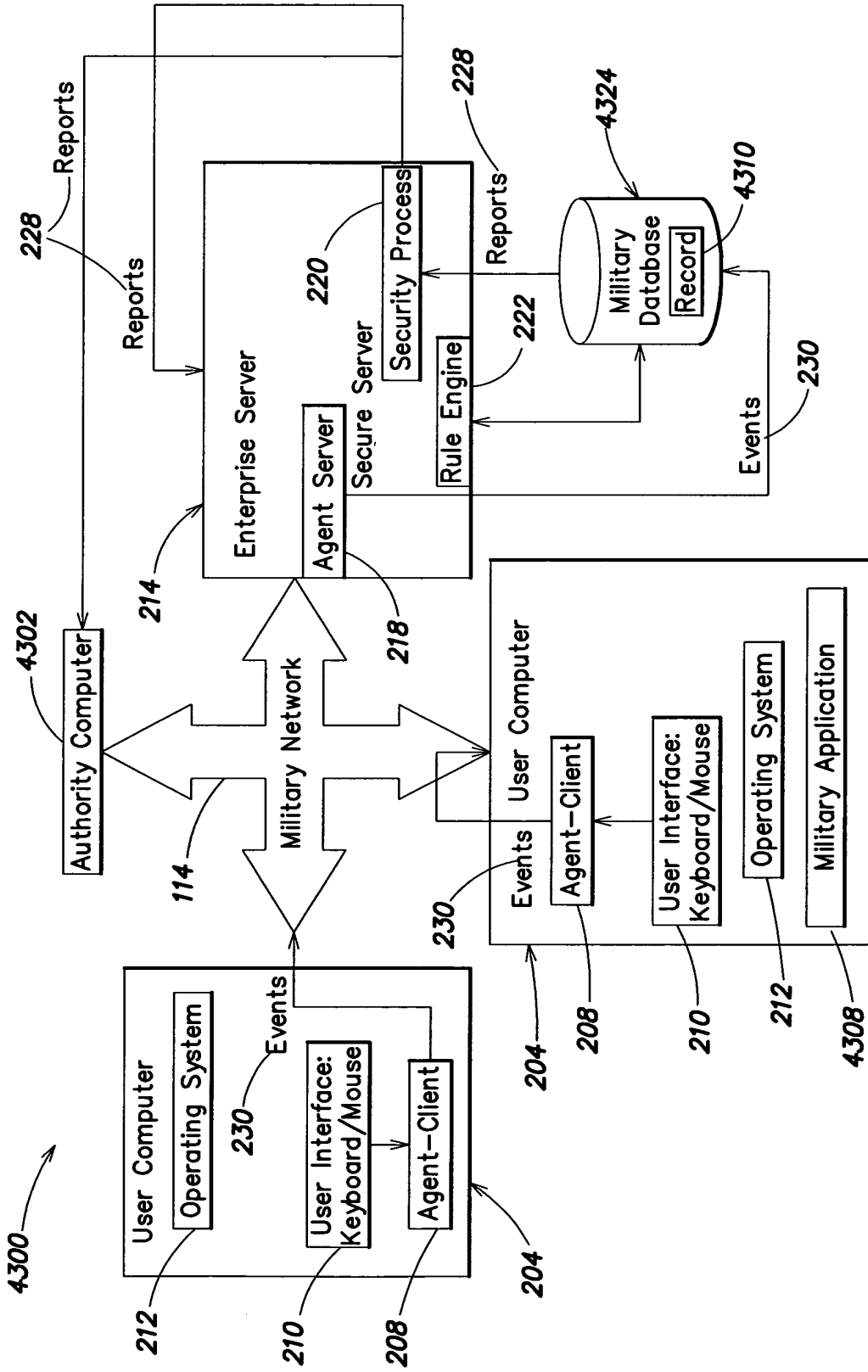


FIG. 43

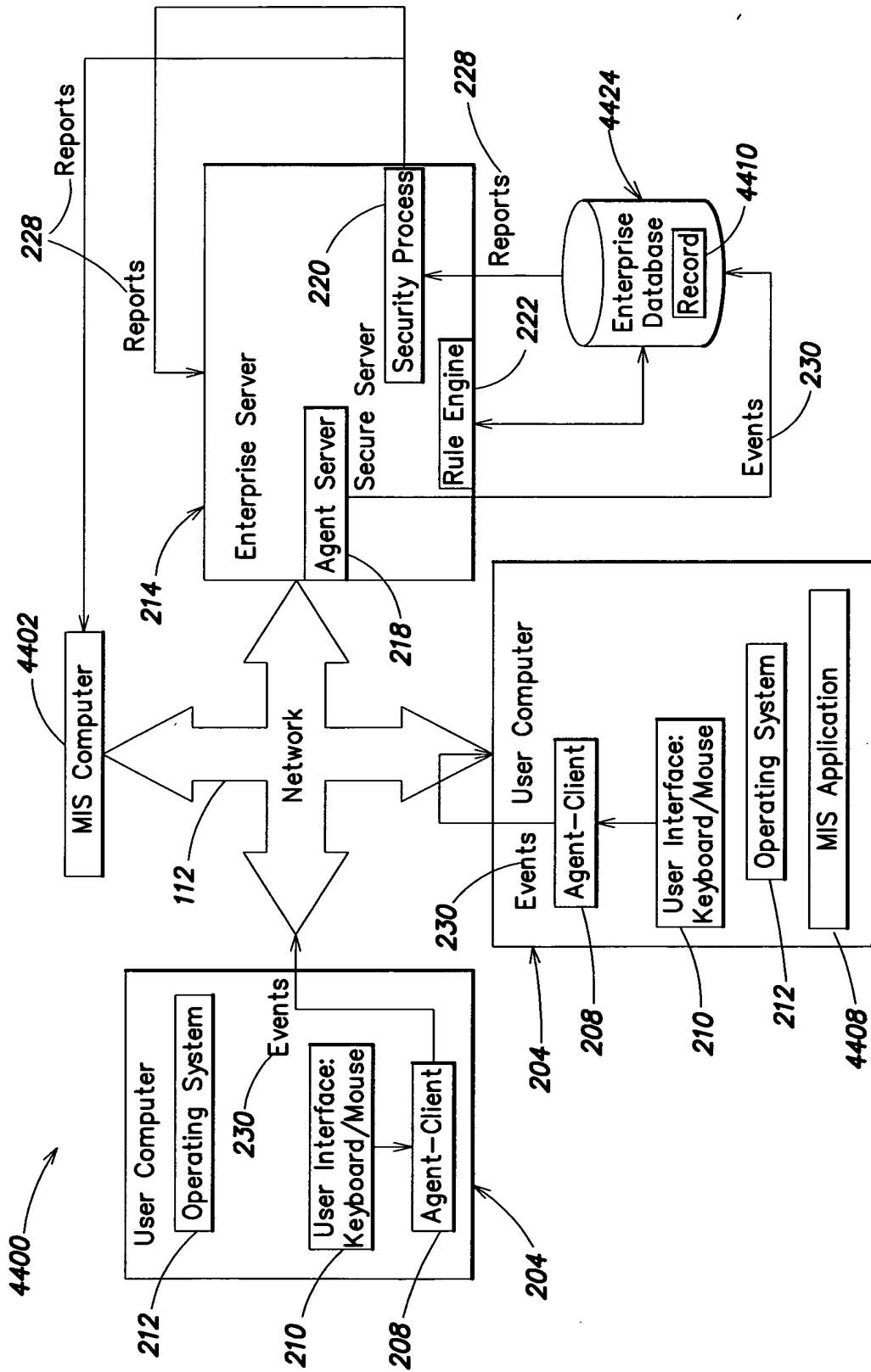


FIG. 44

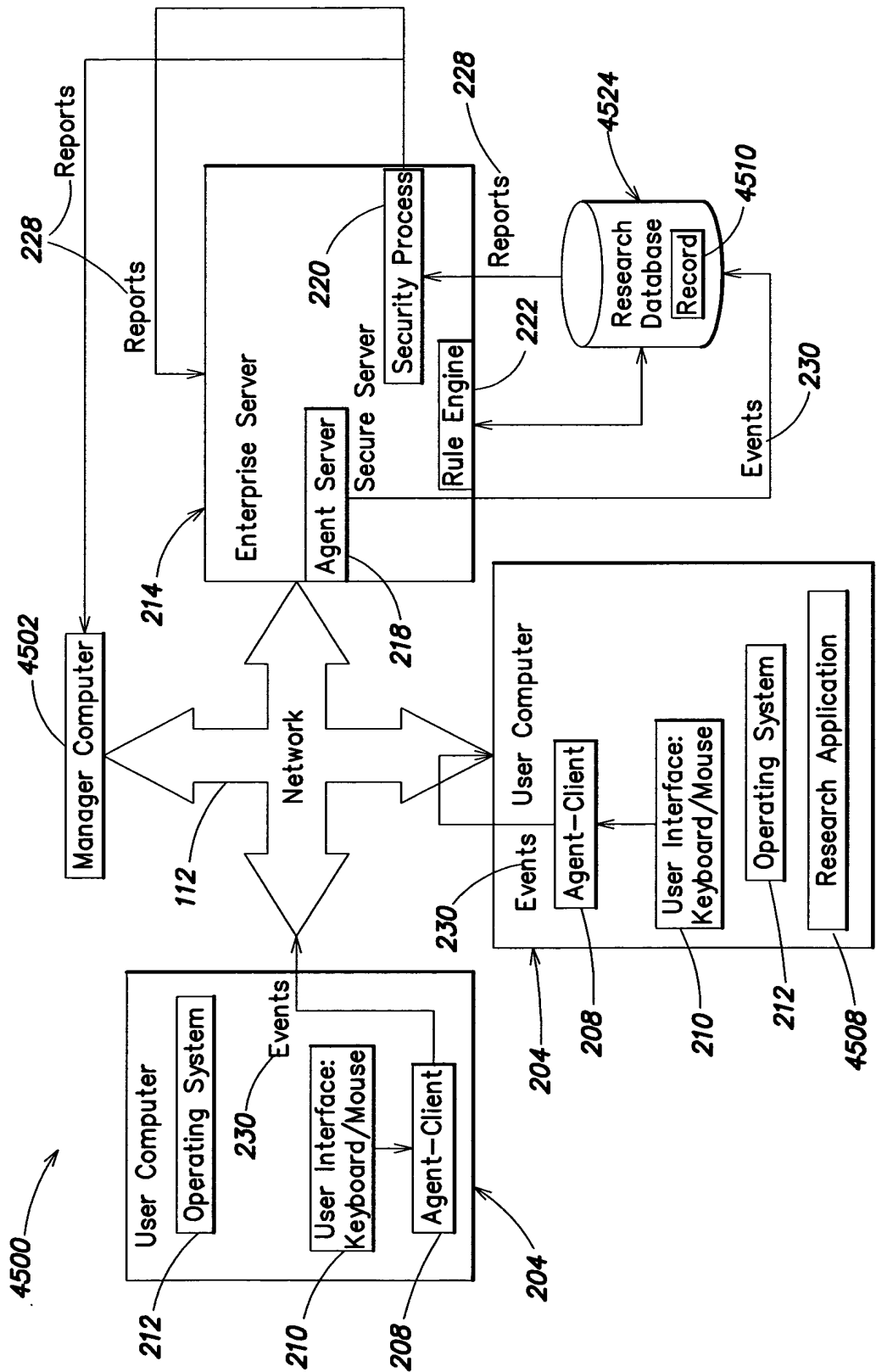


FIG. 45

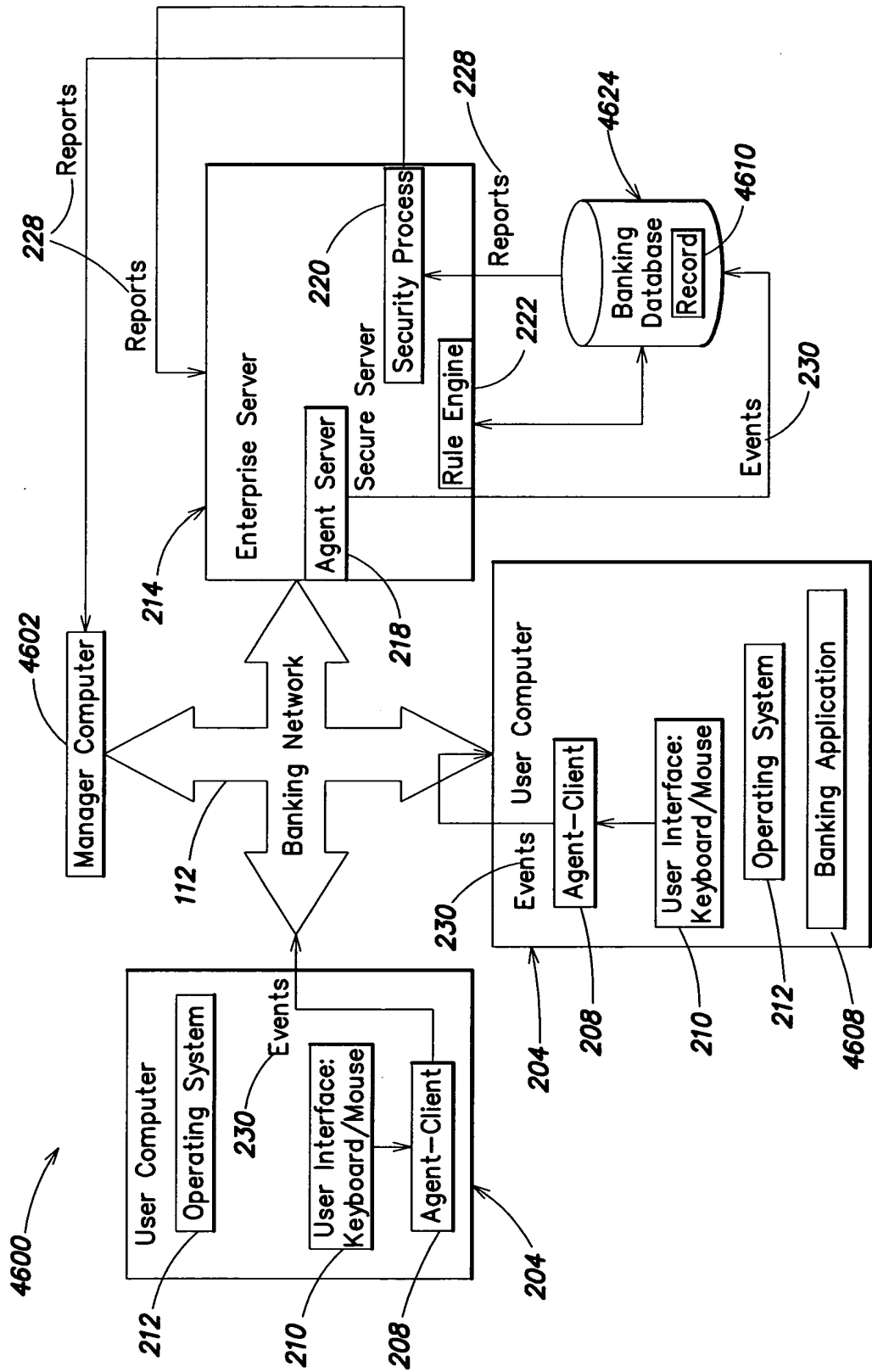


FIG. 46

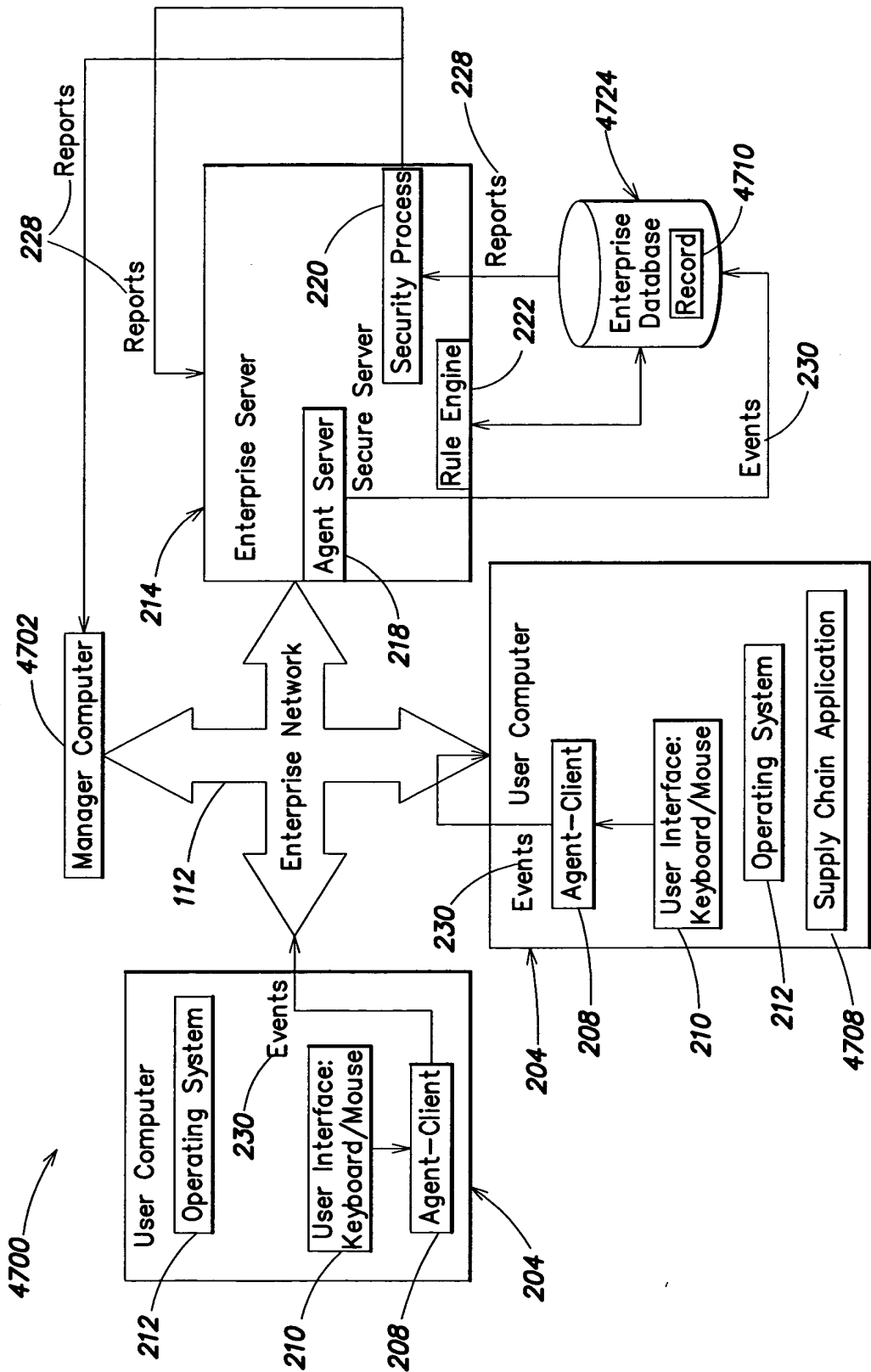


FIG. 47

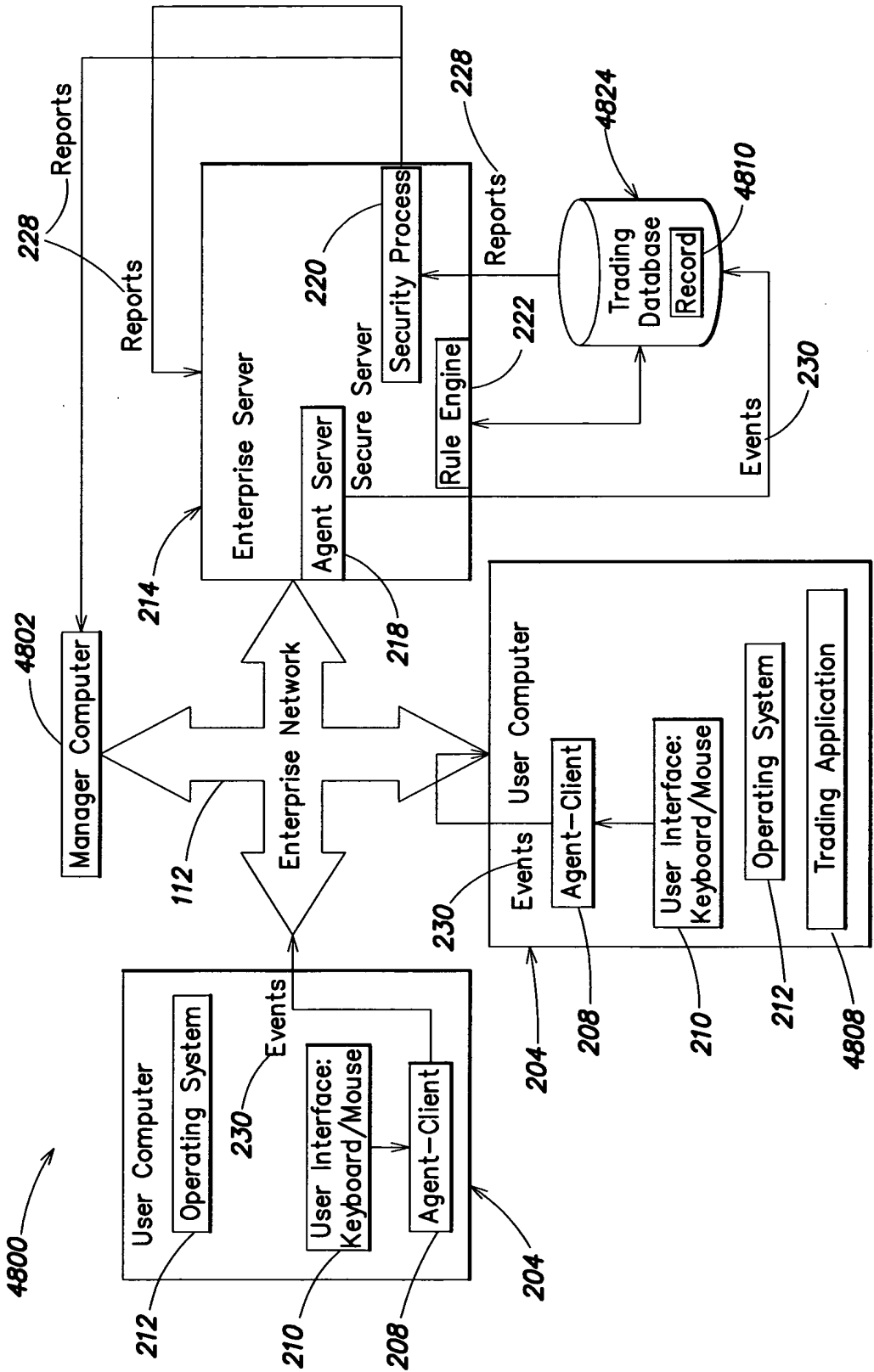


FIG. 48